日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　９月１１日

出願番号
Application Number: 特願２００２－２６５７６９

[ST. 10/C]: [ＪＰ２００２－２６５７６９]

出願人
Applicant(s): パイオニア株式会社

２００３年　７月１０日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎

出証番号　出証特２００３－３０５５６７０

【書類名】　特許願

【整理番号】　57P0161

【提出日】　平成14年 9月11日

【あて先】　特許庁長官殿

【国際特許分類】　G11B 20/10

G06B 13/00

G06F 3/06

【発明者】

【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内

【氏名】　竹村　到

【発明者】

【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内

【氏名】　吉田　和幸

【特許出願人】

【識別番号】　000005016

【氏名又は名称】　パイオニア株式会社

【代理人】

【識別番号】　100079083

【弁理士】

【氏名又は名称】　木下　實三

【電話番号】　03(3393)7800

【選任した代理人】

【識別番号】　100094075

【弁理士】

【氏名又は名称】　中山　寛二

【電話番号】　03(3393)7800

【選任した代理人】

【識別番号】　100106390

【弁理士】

【氏名又は名称】　石崎　剛

【電話番号】　03(3393)7800

【手数料の表示】

【予納台帳番号】　021924

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　情報記録媒体、情報記録装置、情報再生装置、情報配信装置、それらの方法、それらのプログラムおよびそのプログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　コンテンツ暗号鍵を利用して暗号化されたコンテンツと、前記暗号化されたコンテンツを復号化するために利用されかつ復号鍵用暗号鍵で暗号化されたコンテンツ復号鍵とが記録されているとともに、

前記復号鍵用暗号鍵は、少なくともコンテンツ再生の許可・不許可を制御するために予め設定された地域毎に異なる鍵であり、前記コンテンツ暗号鍵および前記コンテンツ復号鍵は、コンテンツ再生が許可された地域毎またはコンテンツ再生が許可された地域の組合せに対応して設定されていることを特徴とする情報記録媒体。

【請求項２】　請求項１に記載の情報記録媒体において、

前記コンテンツ復号鍵は、コンテンツ再生が許可された再生装置に対応して設けられた１つ以上の復号鍵用暗号鍵で暗号化されたものがそれぞれ記録されていることを特徴とする情報記録媒体。

【請求項３】　請求項１または２に記載の情報記録媒体において、

前記復号鍵用暗号鍵の種類を示すヘッダー情報がさらに記録されていることを特徴とする情報記録媒体。

【請求項４】　請求項１ないし３のいずれかに記載の情報記録媒体において、

前記コンテンツ暗号鍵および前記コンテンツ復号鍵は、さらに、コンテンツ再生が許可された地域に属し、かつコンテンツ再生が許可されている再生装置の組合せに対応して設定されていることを特徴とする情報記録媒体。

【請求項５】　請求項１ないし３のいずれかに記載の情報記録媒体において、

前記コンテンツ暗号鍵および前記コンテンツ復号鍵は、所定の再生装置におけるコンテンツ再生を新たに不許可にする場合に新しい鍵に更新されることを特徴とする情報記録媒体。

【請求項６】　請求項１ないし５のいずれかに記載の情報記録媒体において、

前記復号鍵用暗号鍵は、前記各地域毎に独立して設けられた１つ以上の木構造を用いた鍵管理方式で管理されていることを特徴とする情報記録媒体。

【請求項７】　請求項６に記載の情報記録媒体において、

前記復号鍵用暗号鍵は、前記各地域毎に独立して設けられた１つの地域別暗号鍵をルートとし、各再生装置毎に設けられた再生装置別暗号鍵をリーフとする木構造を前記各地域毎に１つ以上設けた鍵管理方式で管理されていることを特徴とする情報記録媒体。

【請求項８】　請求項６または請求項７に記載の情報記録媒体において、

前記各木構造は、ｎ分木（ｎ≧２）が用いられていることを特徴とする情報記録媒体。

【請求項９】　請求項６ないし８のいずれかに記載の情報記録媒体において、

前記復号鍵用暗号鍵は、前記各地域毎に１つずつ設けられた地域別暗号鍵をルートとし、各再生装置毎に設けられた再生装置別暗号鍵をリーフとする完全二分木構造を用いた鍵管理方式で管理されていることを特徴とする情報記録媒体。

【請求項１０】　コンテンツの再生が許可された地域毎またはコンテンツ再生が許可された地域の組合せに対応してコンテンツ暗号鍵を設定して入力するコンテンツ暗号鍵入力手段と、

前記コンテンツ暗号鍵で暗号化されたコンテンツを復号するために利用されるコンテンツ復号鍵を設定して入力するコンテンツ復号鍵入力手段と、

コンテンツの再生が許可された地域に対応する復号鍵用暗号鍵を選択する復号鍵用暗号鍵選択手段と、

前記コンテンツ暗号鍵を利用してコンテンツを暗号化するコンテンツ暗号化手段と、

前記コンテンツ復号鍵を前記復号鍵用暗号鍵を用いて暗号化するコンテンツ復号鍵暗号化手段と、

少なくとも前記暗号化されたコンテンツおよび前記暗号化されたコンテンツ復

号鍵を情報記録媒体に記録する記録手段と、

を備えることを特徴とする情報記録装置。

【請求項１１】　コンテンツ暗号鍵を利用して暗号化されたコンテンツと、前記暗号化されたコンテンツを復号化するために利用されかつ復号鍵用暗号鍵で暗号化されたコンテンツ復号鍵とを有する情報を再生する情報再生装置であって、

前記復号鍵用暗号鍵によって暗号化されたコンテンツ復号鍵を復号する復号鍵用復号鍵が記憶された復号鍵記憶手段と、

前記復号鍵用復号鍵を用いて前記コンテンツ復号鍵を復号するコンテンツ復号鍵復号手段と、

前記コンテンツ復号鍵を利用してコンテンツを復号するコンテンツ復号手段と、

復号されたコンテンツを再生する再生手段とを備え、

前記復号鍵用復号鍵は、少なくともコンテンツ再生の許可・不許可を制御するために予め設定された地域毎に異なる鍵であり、前記コンテンツ暗号鍵および前記コンテンツ復号鍵は、コンテンツ再生が許可された地域毎またはコンテンツ再生が許可された地域の組合せに対応して設定されていることを特徴とする情報再生装置。

【請求項１２】　請求項１１に記載の情報再生装置において、

前記復号鍵記憶手段には、情報再生装置が属する地域に対応して設けられた地域別復号鍵と、情報再生装置毎に割り当てられた再生装置別復号鍵とを含む複数種類の復号鍵用復号鍵が記憶されていることを特徴とする情報再生装置。

【請求項１３】　請求項１２に記載の情報再生装置において、

前記複数種類の復号鍵用復号鍵は、各地域毎に独立して設けられた１つ以上の木構造を用いた鍵管理方式で管理されたものが各再生装置に割り当てられて記憶されていることを特徴とする情報再生装置。

【請求項１４】　請求項１３に記載の情報再生装置において、

前記復号鍵用復号鍵は、前記各地域毎に独立して設けられた１つの地域別復号鍵をルートとし、各再生装置毎に設けられた再生装置別復号鍵をリーフとする木

構造を前記各地域毎に１つ以上設けた鍵管理方式で管理されていることを特徴とする情報再生装置。

【請求項１５】　請求項１ないし９のいずれかに記載の情報記録媒体と、

この情報記録媒体に記憶された前記暗号化されたコンテンツおよび前記暗号化されたコンテンツ復号鍵を配信する配信手段と、

を備えることを特徴とする情報配信装置。

【請求項１６】　コンテンツの再生を許可する地域の選択情報を取得し、

選択された地域またはその組み合わせに対応してコンテンツ暗号鍵およびコンテンツ復号鍵を設定し、

前記選択された地域に対応して予め設定されている復号鍵用暗号鍵を取得し、

前記コンテンツ暗号鍵を利用してコンテンツを暗号化し、

前記コンテンツ復号鍵を前記復号鍵用暗号鍵を用いて暗号化し、

前記暗号化されたコンテンツおよび前記暗号化されたコンテンツ復号鍵を情報記録媒体に記録することを特徴とする情報記録方法。

【請求項１７】　請求項１６に記載の情報記録方法において、

前記復号鍵用暗号鍵は、選択された地域内で再生が許可されている再生装置が保有する復号鍵用暗号鍵は含まれ、再生が許可されていない再生装置が保有する復号鍵用暗号鍵は含まれない復号鍵用暗号鍵の集合の中で最も数が少なくなる組合せで設定することを特徴とする情報記録方法。

【請求項１８】　コンテンツ暗号鍵を利用して暗号化されたコンテンツと、前記暗号化されたコンテンツを復号化するために利用されかつ復号鍵用暗号鍵で暗号化されたコンテンツ復号鍵とを有する情報を再生する情報再生方法であって、

前記復号鍵用復号鍵は、少なくともコンテンツ再生の許可・不許可を制御するために予め設定された地域毎に異なる鍵であり、前記コンテンツ暗号鍵および前記コンテンツ復号鍵は、コンテンツ再生が許可された地域毎またはコンテンツ再生が許可された地域の組合せに対応して設定されているとともに、

前記コンテンツ復号鍵を暗号化した復号鍵用暗号鍵に対応する復号鍵用復号鍵を情報再生装置が保有しているかを調べ、

情報再生装置が対応する復号鍵用復号鍵を保有している場合には、その復号鍵用復号鍵によって前記コンテンツ復号鍵を復号し、

この復号されたコンテンツ復号鍵を利用して前記コンテンツを復号し、

復号されたコンテンツを再生することを特徴とする情報再生方法。

【請求項１９】　コンピュータに、請求項１６または１７に記載の情報記録方法を実行させることを特徴とする情報記録プログラム。

【請求項２０】　コンピュータに、請求項１８に記載の情報再生方法を実行させることを特徴とする情報再生プログラム。

【請求項２１】　請求項１９に記載の情報記録プログラムが、コンピュータにて読取可能に記録されたことを特徴とする情報記録プログラムを記録した記録媒体。

【請求項２２】　請求項２０に記載の情報再生プログラムが、コンピュータにて読取可能に記録されたことを特徴とする情報再生プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報記録媒体、情報記録装置、情報再生装置、情報配信装置、それらの方法、それらのプログラムおよびそのプログラムを記録した記録媒体に関する。

【０００２】

【従来技術】

音楽、映像等のマルチメディアデータ等のコンテンツ（情報、データ）を記録した記録メディア（情報記録媒体）として、ＤＶＤ（Digital Versatile Disc）等の光ディスクが利用されている。このような光ディスクでは、コンテンツの著作権保護のため、リージョンコード（リージョナルコード）と呼ばれる地域固有のフラグを用いてその記録メディアを再生できる地域を限定する方法が採用されている。

すなわち、光ディスクと光ディスクに記録された情報を再生する再生装置（再

生機器や再生ソフトウェア）の両方に、リージョンコードを保有させておく。そして、再生装置は、光ディスクを再生する際に、光ディスクに存在するリージョンコードを読み込み、自分が保有するリージョンコードと一致する場合のみ再生を許可することで、再生地域を限定している。

【０００３】

また、このような光ディスクに記録されたコンテンツは、デジタルデータであるためにコピーしてもデータが劣化することがなく、光ディスクから不正にコピーしたコンテンツが流通すると、著作権者に多大な損害を与えてしまう。このため、前記再生地域を限定するためのリージョンコードとは別に、光ディスクに記録されるコンテンツ自体を暗号化して不正にコピーなどしてもそのデータを閲覧できないようにして、著作権保護を図る技術も近年、採用されるようになった。

【０００４】

具体的には、光ディスクに記録するコンテンツを予め所定の暗号鍵で暗号化し、再生装置が保有する復号鍵を用いて暗号化された前記コンテンツを復号して再生するようにしている。

この際、著作権保護の実効を図るためには、復号鍵が漏洩した再生装置等、特定の再生装置でのコンテンツの再生の許可・不許可をメディア側でコントロールできるようにする必要がある。このため、前記復号鍵を各再生装置毎に異なるものとし、コンテンツの再生を不許可つまりその再生装置を無効化する場合には、その再生装置が保有する復号鍵では復号できない暗号鍵でコンテンツを暗号化し、光ディスクに記録すればよい。

ここで、暗号鍵およびコンテンツを１対１で対応させる方法もあるが、特定の再生装置を無効化するためなどのセキュリティ等の要求により、複数の暗号鍵を用いる必要がある場合、各暗号鍵で暗号化した各コンテンツすべてを記録媒体に記録しなければならず、記録容量の点で問題があった。

【０００５】

このため、コンテンツを復号する復号鍵をさらに別の暗号鍵で暗号化し、この暗号鍵を復号するための復号鍵を各再生装置に予め組み込んでおく方法が用いられるようになった。

但し、この場合でも、各再生装置に１つの復号鍵しか記録されていない場合には、光ディスクには全ての再生装置の持つ復号鍵に対応する暗号鍵でコンテンツ復号鍵を暗号化して記録しなければならないため、暗号化された各コンテンツ復号鍵の個々のサイズは小さくても、再生装置の数が膨大になるとそのデータ容量も膨大になるため、現実的には利用することができない。

【０００６】

このため、光ディスクに記録する暗号化されたコンテンツ復号鍵の数を減らすことを目的として、木構造等を用いて階層的に管理される復号鍵を予め複数用意しておき、各再生装置には複数の復号鍵を、その組合せが各再生装置毎に異なるように記録していた。

このような仕組みを採用しておくことで、仮に特定の再生装置で使用していた復号鍵が漏洩した場合には、コンテンツが記録された新たな光ディスクを製造する際に、その特定の再生装置が備えていない復号鍵に対応する暗号鍵を用いることで、その特定の再生装置でのコンテンツの再生を防止することができ、鍵漏洩時の損害を最小限に抑えることができるという利点がある。

但し、このような方式では、光ディスクに記録する暗号化されたコンテンツ用復号鍵の数を減らすことができるが、一方で、再生装置毎に１つの復号鍵のみを記録する場合に比べて多数の鍵を管理しなければならない。すなわち、光ディスクには各復号鍵に対応する暗号鍵で暗号化されたコンテンツ用復号鍵をそれぞれ記録しておく必要がある。また、再生装置側にも、多数の復号鍵を記録しておく必要がある。

【０００７】

このような複数の鍵の管理を効率的に行う方法として、木構造の鍵管理方式を応用した以下の文献１，２がある。

文献１：「D.Naor, M.Naor, and J.Lotspiech, ”Revocation and Tracing Scheme for Stateless Receivers,” Proceedings of CRYPTO2001, Lecture Notes in Computer Science, Vol.2139, pp.41-62, 2001」

文献２：「中野稔久，大森基司，松崎なつめ，館林誠，”デジタルコンテンツ保護用鍵管理方式-木構造パターン分割方式-,” 2002年暗号と情報セキュリティ

シンポジウム講演論文集,pp715-720」

【０００８】

文献１には、木構造を用いた鍵管理方式の一つであるComplete Subtree Methodが記載されている。この方法では、図１に示すように、各リーフ（木構造における最下位層に位置するノード）には再生装置が１つずつ割り当てられている。また、ルート（木構造における最上位層に位置するノード）とリーフを含む各ノードには、それぞれ暗号鍵BE_iとそれに対応する復号鍵BD_iが１つずつ割り当てられている。なお、暗号鍵BE_iと復号鍵BD_iとは、暗号鍵BE_iを用いて暗号化した暗号文を、同じ添え字「$_i$」の復号鍵BD_iを有する再生装置で復号することができる関係にあり、１対１に対応するものである。このため、図１では、代表して復号鍵BD_iのみを表示し、対応する暗号鍵BE_iを省略している。

一方、各再生装置には、自身が割り当てられたノードからルートに至るパス上に存在する復号鍵BD_iが予め配布されている。

図１に示す例では、再生装置は１６台設けられており、各再生装置１～１６がそれぞれ保有しておく復号鍵BD_iは５つになる。例えば、再生装置４は、図１において丸で囲まれている５つの復号鍵BD_1, BD_2, BD_4, BD_9, BD_{19}を備えている。一般的に、再生装置が保有する復号鍵BD_iの数は、再生装置の総数をＮとすると$\log_2 N+1$となる。

【０００９】

そして、すべての再生装置１～１６に再生許可を与える場合には、メディア４０１にはEncryption（コンテンツ復号鍵AD, 暗号鍵BE_1）、Encryption（コンテンツ, コンテンツ暗号鍵AE）を記録しておけばよい。ここで、Encryption ()は暗号化アルゴリズムを表し、Encryption（引数１, 引数２）は引数２を暗号鍵として引数１を暗号化した暗号文を表す。

従って、メディア４０１には、コンテンツ暗号鍵AEで暗号化されたコンテンツと、暗号鍵BE_1で暗号化されたコンテンツ復号鍵ADとが記録されていることになる。暗号鍵BE_1に対応する復号鍵BD_1は、すべての再生装置１～１６が保有しているため、各再生装置１～１６は、メディア４０１を再生する際には、保有する復号鍵BD_1を用いてコンテンツ復号鍵ADを復号し、次に、このコンテンツ復号鍵AD

を用いてコンテンツを復号してコンテンツを再生する。

【００１０】

一方、ある特定（１つあるいは複数）の再生装置を無効化（その再生装置でコンテンツが再生できないようにメディアを設定）したい場合には、まず、コンテンツを暗号化するための新しいコンテンツ暗号鍵AE_2と、それに対応するコンテンツ復号鍵AD_2を用意し、コンテンツはこの新しいコンテンツ暗号鍵AE_2を用いて暗号化する。

【００１１】

次に、無効化したい再生装置を除く全ての再生装置をカバーできるような部分木の中で、その数が最小となるような部分木を構成する。そして、その部分木のルートに割り当てられている暗号鍵BE_iで、前記コンテンツ復号鍵AD_2を暗号化する。

例えば、図２に示すように、再生装置４を無効化する場合には、再生装置４が保有する復号鍵が含まれないように、復号鍵BD_3, BD_5, BD_8, BD_{18}を用いてコンテンツ復号鍵AD_2を暗号化する。

そして、前記暗号化されたコンテンツ＝Encryption（コンテンツ，コンテンツ暗号鍵AE_2）と、暗号化されたコンテンツ復号鍵AD_2＝Encryption（コンテンツ復号鍵AD_2，暗号鍵BE_3)|Encryption（コンテンツ復号鍵AD_2，暗号鍵BE_5)|Encryption（コンテンツ復号鍵AD_2，暗号鍵BE_8)|Encryption（コンテンツ復号鍵AD_2，暗号鍵BE_{18})を新たなメディア４０２に記録する。なお、記号｜は、二つのデータの結合を表す。

【００１２】

以上により、新たなメディア４０２は、再生装置４では再生できず、他の再生装置では再生可能となる。

なお、この場合、メディア４０２に記録される暗号化されたコンテンツ復号鍵AD_2の数は、メディア４０１に比べて多くなるが、その数の上限は、無効化したい再生装置の数をｒ、再生装置の総数をＮとした場合、$r\log_2(N/r)$で表される。但し、コンテンツ復号鍵のデータ容量はコンテンツに比べて非常に小さいため、その数がある程度増えても記憶容量的にはそれほど問題とならない。

【００１３】

文献２の方法は、木構造パターン分割方式と呼ばれる方法であり、木構造の各レイヤにおける複数のノードに対し、その子ノードに無効化すべき再生装置が存在しているノードを「１」、存在しないノードを「０」で表す。そして、これらの値を木構造の左から順に結合してノード無効化パターンを作成し、このノード無効化パターン毎に異なる暗号鍵（復号鍵）を割り当てることで、再生機器が保有する復号鍵の増加を抑えつつ、記録媒体に記録する鍵情報サイズを小さくしたものである。

【００１４】

これらの各文献１，２に記載された技術は、特定の再生装置における復号鍵の無効化に用いられ、リージョンコードによる地域限定の再生機能とはまったく別に用いられていた。

【００１５】

【発明が解決しようとする課題】

上述したリージョンコードを用いた従来技術の場合、光ディスク等の記録メディアと再生装置とのリージョンコードが一致するかを比較しているだけであるため、メディア側または再生装置側のリージョンコードを違法に書き換えたり、再生装置側のリージョンコード比較装置を取り除くことで、どの地域でも再生可能なメディアや再生装置が比較的容易にできてしまうという課題が一例として挙げられる。

【００１６】

また、上記文献１，２のような木構造の鍵管理方式を用いて特定の再生装置を無効化する技術の場合、リージョンコードのような地域を限定した再生機能を備えていないため、再生を許可する地域を限定する場合にはリージョンコードを併用しなければならず、リージョンコードを用いた場合の課題も発生してしまうという課題が一例として挙げられる。

さらに、暗号鍵や復号鍵が破られた場合には、すべての記録媒体において、コンテンツ復号鍵やコンテンツ暗号鍵を修正しなければならず、対応が困難であるという課題が一例として挙げられる。

【００１７】

本発明は、上述した実情に鑑みて、再生地域を限定できて著作権保護機能を高めることができる情報記録媒体、情報記録装置、情報再生装置、情報配信装置、それらの方法、それらのプログラムおよびそのプログラムを記録した記録媒体を提供することを目的とする。

【００１８】

【課題を解決するための手段】

請求項１に記載の発明は、コンテンツ暗号鍵を利用して暗号化されたコンテンツと、前記暗号化されたコンテンツを復号化するために利用されかつ復号鍵用暗号鍵で暗号化されたコンテンツ復号鍵とが記録されているとともに、前記復号鍵用暗号鍵は、少なくともコンテンツ再生の許可・不許可を制御するために予め設定された地域毎に異なる鍵であり、前記コンテンツ暗号鍵および前記コンテンツ復号鍵は、コンテンツ再生が許可された地域毎またはコンテンツ再生が許可された地域の組合せに対応して設定されていることを特徴とする情報記録媒体である。

【００１９】

請求項１０に記載の発明は、コンテンツの再生が許可された地域毎またはコンテンツ再生が許可された地域の組合せに対応してコンテンツ暗号鍵を設定して入力するコンテンツ暗号鍵入力手段と、前記コンテンツ暗号鍵で暗号化されたコンテンツを復号するために利用されるコンテンツ復号鍵を設定して入力するコンテンツ復号鍵入力手段と、コンテンツの再生が許可された地域に対応する復号鍵用暗号鍵を選択する復号鍵用暗号鍵選択手段と、前記コンテンツ暗号鍵を利用してコンテンツを暗号化するコンテンツ暗号化手段と、前記コンテンツ復号鍵を前記復号鍵用暗号鍵を用いて暗号化するコンテンツ復号鍵暗号化手段と、少なくとも前記暗号化されたコンテンツおよび前記暗号化されたコンテンツ復号鍵を情報記録媒体に記録する記録手段と、を備えることを特徴とする情報記録装置である。

【００２０】

請求項１１に記載の発明は、コンテンツ暗号鍵を利用して暗号化されたコンテンツと、前記暗号化されたコンテンツを復号化するために利用されかつ復号鍵用

暗号鍵で暗号化されたコンテンツ復号鍵とを有する情報を再生する情報再生装置であって、前記復号鍵用暗号鍵によって暗号化されたコンテンツ復号鍵を復号する復号鍵用復号鍵が記憶された復号鍵記憶手段と、前記復号鍵用復号鍵を用いて前記コンテンツ復号鍵を復号するコンテンツ復号鍵復号手段と、前記コンテンツ復号鍵を利用してコンテンツを復号するコンテンツ復号手段と、復号されたコンテンツを再生する再生手段とを備え、前記復号鍵用復号鍵は、少なくともコンテンツ再生の許可・不許可を制御するために予め設定された地域毎に異なる鍵であり、前記コンテンツ暗号鍵および前記コンテンツ復号鍵は、コンテンツ再生が許可された地域毎またはコンテンツ再生が許可された地域の組合せに対応して設定されていることを特徴とする情報再生装置である。

【００２１】

請求項１５に記載の発明は、請求項１ないし９のいずれかに記載の情報記録媒体と、この情報記録媒体に記憶された前記暗号化されたコンテンツおよび前記暗号化されたコンテンツ復号鍵を配信する配信手段と、を備えることを特徴とする情報配信装置である。

【００２２】

請求項１６に記載の発明は、コンテンツの再生を許可する地域の選択情報を取得し、選択された地域またはその組み合わせに対応してコンテンツ暗号鍵およびコンテンツ復号鍵を設定し、前記選択された地域に対応して予め設定されている復号鍵用暗号鍵を取得し、前記コンテンツ暗号鍵を利用してコンテンツを暗号化し、前記コンテンツ復号鍵を前記復号鍵用暗号鍵を用いて暗号化し、前記暗号化されたコンテンツおよび前記暗号化されたコンテンツ復号鍵を情報記録媒体に記録することを特徴とする情報記録方法である。

【００２３】

請求項１８に記載の発明は、コンテンツ暗号鍵を利用して暗号化されたコンテンツと、前記暗号化されたコンテンツを復号化するために利用されかつ復号鍵用暗号鍵で暗号化されたコンテンツ復号鍵とを有する情報を再生する情報再生方法であって、前記復号鍵用復号鍵は、少なくともコンテンツ再生の許可・不許可を制御するために予め設定された地域毎に異なる鍵であり、前記コンテンツ暗号鍵

および前記コンテンツ復号鍵は、コンテンツ再生が許可された地域毎またはコンテンツ再生が許可された地域の組合せに対応して設定されているとともに、前記コンテンツ復号鍵を暗号化した復号鍵用暗号鍵に対応する復号鍵用復号鍵を情報再生装置が保有しているかを調べ、情報再生装置が対応する復号鍵用復号鍵を保有している場合には、その復号鍵用復号鍵によって前記コンテンツ復号鍵を復号し、この復号されたコンテンツ復号鍵を利用して前記コンテンツを復号し、復号されたコンテンツを再生することを特徴とする情報再生方法である。

【００２４】

請求項１９に記載の発明は、コンピュータに、請求項１６または１７に記載の情報記録方法を実行させることを特徴とする情報記録プログラムである。

【００２５】

請求項２０に記載の発明は、コンピュータに、請求項１８に記載の情報再生方法を実行させることを特徴とする情報再生プログラムである。

【００２６】

請求項２１に記載の発明は、請求項１９に記載の情報記録プログラムが、コンピュータにて読取可能に記録されたことを特徴とする情報記録プログラムを記録した記録媒体である。

【００２７】

請求項２２に記載の発明は、請求項２０に記載の情報再生プログラムが、コンピュータにて読取可能に記録されたことを特徴とする情報再生プログラムを記録した記録媒体である。

【００２８】

【発明の実施の形態】

以下に、本発明の実施の形態を図面に基づいて説明する。

本実施形態は、情報記録媒体である記録メディアに情報（コンテンツ）を記録する情報記録装置としての記録装置１００および記録メディアの情報を再生する情報再生装置としての再生装置２００を備える記録再生システムである。

【００２９】

[記録装置の構成]

本実施形態の記録装置１００の構成を図３のブロック図を参照して説明する。この記録装置１００は、記録メディアとして光ディスク用の原盤１０１にコンテンツを書き込むものである。

なお、図３に示す記録装置１００において、原盤１０１の具体的なカッティング方法（原盤作製方法）や、作製された原盤１０１によってＤＶＤ－ＲＯＭ（Digital Versatile Disc - Read Only Memory）などのあらかじめ情報が記録された再生専用の光ディスク等を製造する方法は、周知の技術であるため、それらについての図示及び詳細な説明は行わない。

【００３０】

記録装置１００は、図３に示すように、データ入力回路１１０と、コンテンツ復号鍵入力手段であるコンテンツ復号鍵入力回路１２０と、コンテンツ暗号鍵入力手段であるコンテンツ暗号鍵入力回路１３０と、コンテンツ暗号化手段であるデータ暗号化回路１４０と、復号鍵用暗号鍵選択手段である鍵暗号鍵入力回路１５０と、コンテンツ復号鍵暗号化手段であるコンテンツ復号鍵暗号化回路１６０と、エラー訂正回路１７０と、記録手段であるメディア記録手段１８０と、を備えている。

なお、各回路１１０，１２０，１３０，１４０，１５０，１６０，１７０は、専用のハードウェアによって構成されていてもよいし、記録装置１００に処理装置（ＣＰＵ）やメインメモリ等のハードウェア資源を設け、このハードウェア資源と前記ＣＰＵに組み込まれて実行されるプログラムとが協働して具現化されるものでもよい。

【００３１】

データ入力回路１１０は、記録メディアである光ディスクに記録するコンテンツを記録装置１００に入力する回路である。コンテンツとしては、通常、音楽、映像等の各種マルチメディアデータであるが、それに限定されるものではなく、通常の文書データ等でもよい。このデータ入力回路１１０は、入力されたコンテンツである信号Ｓ１をデータ暗号化回路１４０に出力する。

このデータ入力回路１１０としては、例えば、コンテンツのマスターデータが記録された磁気テープやＤＶＤ－ＲＷ等の記録メディアを読み込んで信号Ｓ１を

出力する回路や、コンテンツのマスターデータが記録されたコンピュータにＬＡＮやインターネットなどの通信回線を経由してアクセスし、そのデータをダウンロードして読み込んで信号Ｓ１を出力する回路等が利用できる。

なお、信号Ｓ１のデータフォーマットの一例を、図４に示す。信号Ｓ１は、コンテンツ（データ）のみで構成されている。

【００３２】

コンテンツ復号鍵入力回路１２０は、コンテンツ復号用の鍵であるコンテンツ復号鍵AD_Rを入力する回路である。コンテンツ復号鍵入力回路１２０は、入力されたコンテンツ復号鍵AD_Rを信号Ｓ２としてコンテンツ復号鍵暗号化回路１６０に出力する。ここで、コンテンツ復号鍵AD_Rは、コンテンツの再生が許可される地域毎あるいはその地域の組み合わせ毎に異なる値が入力される。具体的には、予め設定された再生許可地域の一覧から、コンテンツの再生を許可する地域を作業者が１つ以上選択すると、コンテンツ復号鍵入力回路１２０は、その選択された地域の組み合わせ（１つの場合も含む）に応じてコンテンツ復号鍵AD_Rを設定し、信号Ｓ２として出力する。

信号Ｓ２のデータフォーマットの一例を、図５に示す。信号Ｓ２は、コンテンツ復号鍵AD_Rのみで構成されている。

【００３３】

なお、再生許可地域は、従来のリージョンコードと同様に、コンテンツ再生の許可・不許可を設定するために、予め設定されるものである。具体的には、リージョンコードに準じて、「北米、日本、ヨーロッパ、アラブ、東南アジア、南アメリカ、オーストラリア、アフリカ、ロシア、南アジア、中国」のような世界の各地域毎に設定してもよい。さらには、より詳細に、各国単位や、国の各地方単位等で設定してもよい。

【００３４】

コンテンツ暗号鍵入力回路１３０は、コンテンツ暗号鍵AE_Rを入力する回路である。コンテンツ暗号鍵入力回路１３０は、入力されたコンテンツ暗号鍵AE_Rを信号Ｓ３としてデータ暗号化回路１４０に出力する。ここで、コンテンツ暗号鍵AE_Rとコンテンツ復号鍵AD_Rは、Ｐ＝Decryption（Encryption（任意のデータＰ，

コンテンツ暗号鍵AE_R），コンテンツ復号鍵AD_R）の関係が成り立つように設定される。従って、コンテンツ復号鍵AD_Rと同様に、コンテンツ暗号鍵AE_Rもコンテンツの再生が許可される地域毎やその組み合わせで設定される。

信号Ｓ３のデータフォーマットの一例を、図６に示す。信号Ｓ３は、コンテンツ暗号鍵AE_Rのみで構成されている。

【００３５】

ここで、Decryption（）は復号化アルゴリズムを表す。そして、Decryption（引数１，引数２）は引数２を復号鍵として引数１を復号したデータを表す。従って、上記Ｐは、任意のデータＰをコンテンツ暗号鍵AE_Rを用いて暗号化した暗号文を、コンテンツ復号鍵AD_Rを用いて復号したデータである。

【００３６】

データ暗号化回路１４０は、信号Ｓ３＝コンテンツ暗号鍵AE_Rを用いて信号Ｓ１＝コンテンツを暗号化し、信号Ｓ４＝Encryption（コンテンツ，コンテンツ暗号鍵AE_R）を出力する回路である。従って、信号Ｓ４は、コンテンツ暗号鍵AE_Rを用いて暗号化されたコンテンツであり、この信号Ｓ４のデータフォーマットの一例を図７に示す。

【００３７】

鍵暗号鍵入力回路１５０は、コンテンツ復号鍵AD_Rを暗号化するための暗号鍵（復号鍵用暗号鍵）BE_iを入力する回路である。ここで、暗号鍵BE_iは、少なくとも、コンテンツ再生の許可・不許可を制御するために予め設定された前記地域毎に異なるものであり、そのコンテンツの再生を許可する地域に応じて選択されて入力される。

このため、複数の地域での再生が許可されている場合等、複数の暗号鍵BE_iが入力されることもあり、例えば、Ｎ個の暗号鍵BE_1，BE_2，…，BE_i，…BE_{N-1}，BE_Nが入力された場合には、鍵暗号鍵入力回路１５０は、信号Ｓ５＝暗号鍵BE_1｜暗号鍵BE_2｜…｜暗号鍵BE_i｜…｜暗号鍵BE_{N-1}｜暗号鍵BE_Nを出力する。従って、信号Ｓ５は鍵暗号鍵入力回路１５０によって入力された複数の暗号鍵BE_iが結合されたデータであり、この信号Ｓ５のデータフォーマットの一例を図８に示す。

【００３８】

コンテンツ復号鍵暗号化回路１６０は、信号Ｓ５に含まれる各暗号鍵BE_iを用いて信号Ｓ２＝コンテンツ復号鍵AD_Rを暗号化し、それにヘッダー情報Header（暗号鍵BE_i）を付加して信号Ｓ６を出力する回路である。

ここで、信号Ｓ６＝Header（暗号鍵BE_1）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_1）｜Header（暗号鍵BE_2）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_2）｜…｜Header（暗号鍵BE_i）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）｜…｜Header（暗号鍵BE_{N-1}）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_{N-1}）｜Header（暗号鍵BE_N）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_N）である。

【００３９】

以下では、簡単に表記するため、信号Ｓ６＝Header（暗号鍵BE_i）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）と表す。すなわち、信号Ｓ６は、図９に示すように、複数の暗号鍵BE_iを用いて暗号化されたコンテンツ復号鍵AD_Rと、そのヘッダー情報Header（暗号鍵BE_i）とで構成されている。

なお、ヘッダー情報Header（暗号鍵BE_i）は、使用した暗号鍵BE_iを識別するために利用される情報である。

【００４０】

エラー訂正回路１７０は、信号Ｓ４＝Encryption（コンテンツ，コンテンツ暗号鍵AE_R）と、信号Ｓ６＝Header（暗号鍵BE_i）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）とを入力とし、それらを結合してエラー訂正符号を付加したものを信号Ｓ７として出力する装置である。

信号Ｓ７は、図１０にも示すように、コンテンツ暗号鍵AE_Rで暗号化されたコンテンツと、Ｎ個の暗号鍵BE_iで暗号化されたＮ個のコンテンツ復号鍵AD_Rと、各暗号鍵BE_iのヘッダー情報と、エラー訂正符号とからなる信号である。つまり、Ｓ７＝Header（暗号鍵BE_i）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）｜Encryption（コンテンツ，コンテンツ暗号鍵AE_R）｜ＥＣＣである。

ここで、ＥＣＣ（Error Correcting Code）はエラー訂正符号を表している。なお、ＥＣＣを用いたエラー訂正の具体的方法は周知の技術であるため、説明を

省略する。

【００４１】

メディア記録手段１８０は、入力された信号Ｓ７を、光ディスク又は光ディスクを製造するための原盤等の記録メディアに記録する装置である。例えば、記録メディアとして原盤１０１が用いられる場合には、原盤カッティング用レーザー発振器がメディア記録手段１８０として利用される。一方、記録メディアとして、ＤＶＤ－Ｒ，ＤＶＤ－ＲＷ，ＤＶＤ－ＲＡＭ、ＣＤ－Ｒ等の記録可能な各種光メディアが用いられる場合には、データ記録用のレーザー発振器がメディア記録手段１８０として利用される。

なお、メディア記録手段１８０によってデータが記録される記録メディアとしては、一般に、光ディスクを大量に生産する場合には原盤１０１が用いられ、オンデマンド生産等の少量生産の場合には、各種記録用の光ディスクが用いられる。

【００４２】

［再生装置の構成］

次に、コンテンツが記録された記録メディアである光ディスクを再生する情報再生装置である再生装置２００の概略構成について、図１１に示すブロック図および図１２～１７のデータフォーマット図を参照して説明する。

再生装置２００は、情報読取手段２１０と、エラー訂正回路２２０と、復号鍵記憶手段である復号鍵記憶装置２３０と、コンテンツ復号鍵復号手段であるコンテンツ復号鍵復号回路２４０と、コンテンツ復号手段であるデータ復号回路２５０と、再生手段であるデコーダ２６０とを備える。そして、記録メディアである光ディスク２０１に記録されたコンテンツを再生し、ディスプレイやスピーカー等の出力装置に出力するものである。

【００４３】

ここで、光ディスク２０１は、前記記録装置１００でデータが記録された原盤１０１を元に製造された記録メディアとしての光ディスク２０１であり、例えばＤＶＤ－ＲＯＭやＣＤ－ＲＯＭである。

なお、各回路２２０，２４０，２５０や復号鍵記憶装置２３０、デコーダ２６

０は、専用のハードウェアによって構成されていてもよいし、再生装置２００に処理装置（ＣＰＵ）やメインメモリ等のハードウェア資源を設け、このハードウェア資源と前記ＣＰＵに組み込まれて実行されるプログラムとが協働して具現化されるものでもよい。

【００４４】

情報読取手段２１０は、光ディスク２０１に記録された情報を読み取る光ピックアップ等の装置であり、信号Ｓ１１を出力する。信号Ｓ１１＝Header（暗号鍵BE_i）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）｜Encryption（コンテンツ，コンテンツ暗号鍵AE_R）｜ＥＣＣは、情報読取手段２１０で光ディスク２０１から読み取られた情報であり、前記信号Ｓ７と同じものである。つまり、信号Ｓ１１は、図１２に示すように、複数の暗号鍵BE_iを用いて暗号化されたコンテンツ復号鍵AD_Rと、各暗号鍵BE_iのヘッダー情報と、コンテンツ暗号鍵AE_Rで暗号化されたコンテンツと、エラー訂正符号ＥＣＣとを備えている。

【００４５】

エラー訂正回路２２０は、入力された信号Ｓ１１のエラー訂正を行う装置である。エラー訂正の方法は、前述の通り、ＥＣＣを用いた周知技術であるため、説明を略す。

エラー訂正回路２２０は、エラー訂正後の信号を信号Ｓ１２＝Header（暗号鍵BE_i）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）と、信号Ｓ１３＝Encryption（コンテンツ，コンテンツ暗号鍵AE_R）とに分けて出力する。

【００４６】

ここで、信号Ｓ１２は、図１３に示すように、信号Ｓ６と同じものである。つまり、暗号鍵BE_iで暗号化されたコンテンツ復号鍵AD_Rと、暗号鍵BE_iのヘッダー情報の集合である。

【００４７】

一方、信号Ｓ１３は、図１４に示すように、コンテンツ暗号鍵AE_Rで暗号化されたコンテンツであり、信号Ｓ４と同じものである。

【００４８】

復号鍵記憶装置２３０は、各再生装置２００が保有する複数種類の復号鍵（復

号鍵用復号鍵）BD_1，BD_2…BD_j…BD_{M-1}，BD_Mと、そのヘッダー情報Header（復号鍵BD_1），Header（復号鍵BD_2），…，Header（復号鍵BD_j），…，Header（復号鍵BD_{M-1}），Header（復号鍵BD_M）を保存しておく装置である。ここでは、M個保有しているとして説明する。

なお、復号鍵記憶装置２３０には、再生装置２００が属する再生地域毎に割り当てられた１つ以上の地域別復号鍵の少なくとも１つと、各再生装置２００毎に割り当てられた再生装置別復号鍵とが、少なくとも保存されている。

【００４９】

復号鍵記憶装置２３０に保存された各復号鍵BD_jは、コンテンツ復号鍵AD_Rの暗号化用の暗号鍵BE_iと、Ｐ＝Decryption（Encryption（任意のデータＰ，暗号鍵BE_i），復号鍵BD_j）の関係が成立するように設定されている。

また、上記関係の暗号鍵BE_iと復号鍵BD_jに付加されたヘッダーについて、Header（暗号鍵BE_i）＝Header（復号鍵BD_j）の関係が成立するようにヘッダーの値が決められている。

【００５０】

復号鍵記憶装置２３０から出力される信号Ｓ１４は、図１５に示すように、復号鍵BD_1｜復号鍵BD_2｜…｜復号鍵BD_j｜…｜復号鍵BD_{M-1}｜復号鍵BD_Mと、そのヘッダー情報Header（復号鍵BD_1）｜Header（復号鍵BD_2）｜…｜Header（復号鍵BD_j）｜…｜Header（復号鍵BD_{M-1}）｜Header（復号鍵BD_M）とを備える。

【００５１】

コンテンツ復号鍵復号回路２４０は、信号Ｓ１２とＳ１４とを入力とし、光ディスク２０１から読み込んだヘッダーHeader（暗号鍵BE_i）と、再生装置２００が保有するヘッダーHeader（復号鍵BD_j）とが一致するか否かを調べ、一致したときは、復号鍵BD_jを用いて暗号化されたコンテンツ復号鍵AD_R＝Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）を復号する回路である。

つまり、コンテンツ復号鍵AD_Rを復号するアルゴリズムは、コンテンツ復号鍵AD_R＝Decryption（Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i），復号鍵BD_j）で表される。

この処理は、一致するヘッダーの組み合わせが見つかるまで各ｉ，ｊの組合せ

について行われ、組合せが見つかってコンテンツ復号鍵AD_Rを復号できた場合には、コンテンツ復号鍵復号回路２４０は、図１６に示すような信号Ｓ１５＝コンテンツ復号鍵AD_Rを出力する。一致する組合せが存在しない場合は、コンテンツ復号鍵復号回路２４０は、信号Ｓ１５を出力できないため、再生装置２００は現在読み込んでいる光ディスク２０１は再生不可能と判断し、すべての処理を終了する。

【００５２】

データ復号回路２５０は、信号Ｓ１３と信号Ｓ１５とを入力とし、信号Ｓ１５を用いて信号Ｓ１３を復号し、その結果であるDecryption（Encryption（コンテンツ，コンテンツ暗号鍵AE_R），コンテンツ復号鍵AD_R）＝コンテンツを、図１７に示すような信号Ｓ１６として出力する回路である。

デコーダ２６０は、入力された信号Ｓ１６＝コンテンツをデコードし、再生する回路である。例えば、再生装置２００がテレビやディスプレイに接続されている場合には、再生されたコンテンツはテレビ等で出力されることになる。

【００５３】

[記録装置の動作]

次に、上記記録装置１００におけるコンテンツ記録時の動作について説明する。

なお、具体的な動作を説明する前に、本実施形態におけるコンテンツの地域限定再生制御機能を有する鍵管理システムに関し、図１８，１９を参照して説明する。

【００５４】

[地域限定再生制御機能付き鍵管理方式]

本方式では、鍵管理用の木を再生地域毎の部分木に分割し、各部分木に一つの再生地域を割り当てている。例えば、図１８に示すように、４つの再生地域１～４が設けられている場合、各再生地域に対応して４つの部分木が設定される。

そして、各部分木のルートおよびリーフを含む各ノードには、暗号鍵BE_iとそれに対応する復号鍵BD_jが一つずつ割り当てられる。そして、各再生装置は、自身が割り当てられたリーフから部分木のルートに至るパス上に存在する復号鍵BD

$_j$を予め保有している。

なお、秘密鍵方式のように、暗号鍵BE_iとそれに対応する復号鍵BD_jとが共通（同一）である場合には、暗号鍵BE_i及び復号鍵BD_jを兼用する１つの鍵を各ノードに割り当てればよい。一方、公開鍵方式のように、暗号鍵BE_iとそれに対応する復号鍵BD_jとが異なる場合には、暗号鍵BE_i及び復号鍵BD_jの２種類の鍵を各ノードに割り当てればよい。なお、図１８，１９では、部分木上には復号鍵BD_jのみを表示し、暗号鍵BE_iを省略している。

【００５５】

ここで、各部分木のルートに割り当てられる暗号鍵BE_4～BE_7および復号鍵BD_4～BD_7は、各再生地域に含まれるすべての再生装置に共通するため、無効化された再生装置が存在しない初期状態で、再生地域を特定するための地域別暗号鍵、復号鍵として機能する。

一方、各部分木のリーフに割り当てられる暗号鍵BE_{16}～BE_{31}および復号鍵BD_{16}～BD_{31}は、各再生装置１～１６で異なるため、再生装置を特定するための再生装置別暗号鍵、復号鍵として機能する。

但し、各暗号鍵BE_{16}～BE_{31}および復号鍵BD_{16}～BD_{31}や、ルート及びリーフの間のノードにある各暗号鍵BE_8～BE_{15}および復号鍵BD_8～BD_{15}も、互いに同一なものがないユニークな鍵であることから、その鍵が特定できればその鍵が対応する再生地域も特定されるため、地域別暗号鍵、復号鍵としても機能する。要するに、地域別暗号鍵や地域別復号鍵とは、その鍵に基づいて対応する再生地域が特定できるものであればよい。

【００５６】

図１８の例では、木構造として完全二分木構造が採用されている。そして、再生装置の総数は１６、再生地域数は４、各再生地域に属する再生装置数は４、各再生装置が保有しておく復号鍵BD_jは３つになる。例えば、再生地域１に所属する再生装置４は、丸で囲まれた３つの復号鍵BD_4，BD_9，BD_{19}を保有している。

これらの各鍵は、各ノード毎に異なるものが割り当てられており、同一の再生地域に属する再生装置間（例えば再生装置１，２間）では、共通する復号鍵（例えば復号鍵BD_4，BD_8）を保有するが、再生地域が異なる再生装置間（例えば再生

装置１，５間）では、共通する復号鍵を保有することがないように設定されている。

なお、再生装置の総数をＮ、再生地域数をＲ、各再生地域には同数の再生装置が存在すると仮定すれば、再生装置が保有する復号鍵BD_jの数は$\log_2(N/R)+1$になる。

【００５７】

そして、例えば、再生地域１のみで再生可能なメディア３０１を作成する場合には、コンテンツ暗号鍵AE_{R1}で暗号化されたコンテンツ＝Encryption（コンテンツ，コンテンツ暗号鍵AE_{R1}）と、再生地域１のルートにある暗号鍵BE_4で暗号化されたコンテンツ復号鍵AD_{R1}＝Encryption（コンテンツ復号鍵AD_{R1}，暗号鍵BE_4）とをメディア３０１に記録しておけばよい。

一方、再生装置３，４のみで再生可能なメディア３０２を作成する場合には、コンテンツ暗号鍵AE_{R34}で暗号化されたコンテンツ＝Encryption（コンテンツ，コンテンツ暗号鍵AE_{R34}）と、再生地域３，４のルートにある暗号鍵BE_6、BE_7でそれぞれ暗号化されたコンテンツ復号鍵AD_{R34}＝Encryption（コンテンツ復号鍵AD_{R34}，暗号鍵BE_6）｜Encryption（コンテンツ復号鍵AD_{R34}，暗号鍵BE_7）とをメディア３０２に記録しておけばよい。

【００５８】

なお、各コンテンツ暗号鍵およびコンテンツ復号鍵のペアは、任意の再生地域の組合せについて一つずつ割り当てられている。すなわち、再生地域１のみに限定されるメディアには、再生地域１用のコンテンツ暗号鍵AE_{R1}，コンテンツ復号鍵AD_{R1}が割り当てられている。一方で、再生地域３，４のみに限定されるメディアには、再生地域３，４の組み合わせ用のコンテンツ暗号鍵AE_{R34}，コンテンツ復号鍵AD_{R34}が割り当てられている。

同様に、再生地域２のみ、３のみ、４のみや、再生地域１，２，３，４用等の各再生地域の組合せに対応して、各コンテンツ暗号鍵およびコンテンツ復号鍵のペアが一つずつ割り当てられている。

【００５９】

ここで、ある再生地域に属する特定（複数または単数）の再生装置を無効化し

たい場合には、無効化したい再生装置の属する部分木のみに対して無効化処理を行えばよい。例えば、再生装置４での再生を無効化したい場合には、図１９に示すように、再生装置４以外の他の再生装置１～３のみがカバーされる部分木を構成し、その部分木の暗号鍵BE_8，BE_{18}を用いて新たに設定（更新）されたコンテンツ復号鍵AD_{2R1}を暗号化し、新たなメディア３０３に記録する。また、このコンテンツ復号鍵AD_{2R1}に対応するコンテンツ暗号鍵AE_{2R1}でコンテンツを暗号化し、新たなメディア３０３に記録する。

これにより、再生装置４では、メディア３０３の暗号鍵BE_8，BE_{18}に対応する復号鍵を保有していないため、メディア３０３のコンテンツ復号鍵AD_{2R1}を復号することができず、このためコンテンツも復号再生することができない。また、復号鍵BD_4，BD_9，BD_{19}のいずれかが漏洩しても、その漏洩した鍵ではメディア３０３は再生できないので、著作権者が保護される。

【００６０】

この際、コンテンツ復号鍵AD_{2R1}およびコンテンツ暗号鍵AE_{2R1}も旧メディア３０１と異なるものとすることで、仮にコンテンツ復号鍵AD_{R1}が漏洩していたとしても、新たなメディア３０３は再生することはできない。

すなわち、コンテンツ復号鍵およびコンテンツ暗号鍵は、新たに無効化すべき再生装置が生じた場合には、新しい鍵に更新された後に設定される。この結果、コンテンツ再生が許可された地域において再生が許可されている（無効化されていない）再生装置の組合せによって異なるコンテンツ復号鍵およびコンテンツ暗号鍵が用いられることになる。従って、再生装置４だけでなく再生装置１も無効化された場合には、さらに新たなコンテンツ復号鍵AD_{3R1}およびコンテンツ暗号鍵AE_{3R1}が用いられる。なお、本実施形態では、各鍵の記号において添え字Ｒの右側に再生地域番号を示し、左側に鍵のバージョンを示している。

【００６１】

この方式の特徴として、再生が許可された地域毎やその地域の組み合わせ毎に異なるコンテンツ復号鍵AD_R、コンテンツ暗号鍵AE_Rを用い、かつ再生装置の保有する復号鍵BD_jや対応する暗号鍵BE_iを管理する部分木が再生地域ごとに独立しているため、ある特定の再生地域のコンテンツ復号鍵AD_Rや、その再生地域に属す

る再生装置の保有する復号鍵BD_jが漏洩しても、影響を受けるのはその再生地域での再生を許可しているメディアのみであり、他の再生地域で再生を許可しているメディアには何の影響も及ぼさない点がある。

図１８，１９の例では、再生装置４の保有する鍵の漏洩の影響を受けるのは、再生地域１を含む再生地域で再生を許可しているメディア３０１のみである。

従って、再生地域３，４限定のメディア３０２は、再生装置４の無効化の有無に関係なく、内容は全く同一のままでよい。

なお、本実施形態では、各再生装置毎に異なる復号鍵BD_jを割り当てており、メディア側に記録する暗号鍵BE_iを変更するだけで各再生装置の無効化を制御できるため、各再生装置１～１６は、保有する鍵の漏洩の有無に関係なく、保有する復号鍵BD_jを何ら変更する必要がない。

【００６２】

[記録装置におけるコンテンツ記録手順]

次に、本実施形態の記録装置１００におけるコンテンツ記録手順について、図２０のフローチャートを参照して説明する。

記録装置１００は、コンテンツを原盤１０１に記録する際に、まず、メディア再生許可地域の選択を促す（ステップＳＴ１）。この選択は、通常、メディアを作成するコンテンツ提供者（著作権者）等が指示、入力することで行われる。

メディア再生許可地域が選択されて記録装置１００がその選択情報を取得すると、コンテンツ暗号鍵入力回路１３０および復号鍵入力回路１２０は、再生対象となる地域の組み合わせに対応したコンテンツ暗号鍵AE_R，コンテンツ復号鍵AD_Rを選択（選定）する（ステップＳＴ２）。例えば、図１８の例では、再生地域３，４が選択されると、その組合せに対応するコンテンツ暗号鍵AE_{R34}、コンテンツ復号鍵AD_{R34}が選択される。

この選択された各鍵は、信号Ｓ３，Ｓ４としてデータ暗号化回路１４０、コンテンツ復号鍵暗号化回路１６０にそれぞれ出力される。

【００６３】

次に、鍵暗号鍵入力回路１５０は、再生許可地域内において対象メディアの再生を許可する再生装置の選択を促す（ステップＳＴ３）。この選択も、通常は、

コンテンツ提供者が行うものであり、例えば、記録装置１００に設けられたディスプレイ等の表示装置（出力装置）とキーボード等の入力装置を用いて、再生許可地域内のすべての再生装置の選択や、特定の再生装置の選択を指示すればよい。なお、復号鍵BD_jが漏洩した再生装置を特定する情報を記憶しておき、復号鍵BD_jが漏洩した再生装置以外という選択肢を用意し、利用者がそれ以外の再生装置を容易に選択できるような構成を採用してもよい。

【００６４】

再生地域と再生装置が選択されると、鍵暗号鍵入力回路１５０は、復号鍵BD_jを選択して所定の復号鍵BD_jの集合を作成する（ステップＳＴ４）。具体的には、選択されたすべての再生装置は、前記集合の中の少なくとも一つの復号鍵BD_jを保有し、選択されなかった（再生が許可されていない）再生装置は前記集合の復号鍵BD_jを一つも保有していないような復号鍵BD_jの集合のうち、その鍵の数が最小となるような集合を選定する。

また、鍵暗号鍵入力回路１５０は、復号鍵BD_jの選択に伴い、選択された復号鍵BD_jに対応する暗号鍵BE_iも選択する（ステップＳＴ４）。

そして、鍵暗号鍵入力回路１５０は、選択された暗号鍵BE_iを信号Ｓ５としてコンテンツ復号鍵暗号化回路１６０に出力する。

【００６５】

コンテンツ復号鍵暗号化回路１６０は、信号Ｓ２，Ｓ５を受け取ると、信号Ｓ２＝コンテンツ復号鍵AD_Rを、信号Ｓ５＝選択されたすべての暗号鍵BE_iを用いて暗号化し、その暗号化されたデータ＝Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）および各暗号鍵BE_iのヘッダー情報からなる信号Ｓ６をエラー訂正回路１７０に出力する（ステップＳＴ５）。

【００６６】

また、データ暗号化回路１４０は、信号Ｓ１と信号Ｓ３とを受け取ると、信号Ｓ１＝コンテンツを、信号Ｓ３＝コンテンツ暗号鍵AE_Rを用いて暗号化し、その暗号化されたデータ＝Encryption（コンテンツ，コンテンツ暗号鍵AE_R）を信号Ｓ４としてエラー訂正回路１７０に出力する（ステップＳＴ６）。

【００６７】

エラー訂正回路１７０は、信号Ｓ４，Ｓ６を受け取ると、各信号Ｓ４，Ｓ６を結合するとともに、エラー訂正符号を付加し、信号Ｓ７としてメディア記録手段１８０に出力する（ステップＳＴ７）。

メディア記録手段１８０は、受け取った信号Ｓ７を記録メディアである原盤１０１に記録する（ステップＳＴ８）。

以上のステップＳＴ１～ＳＴ８によって、所定の再生地域および再生装置でのみ再生可能なメディア（またはその原盤）が生産される。

【００６８】

[再生装置におけるコンテンツ再生手順]

次に、前記記録装置１００で作成されたメディアを再生装置２００で再生する場合の手順について、図２１のフローチャートを参照して説明する。

再生装置２００は、記録メディアである光ディスク２０１がセットされると、情報読取手段２１０により光ディスク２０１の情報を読み取り、その情報を信号Ｓ１１としてエラー訂正回路２２０に出力する（ステップＳＴ１１）。

【００６９】

エラー訂正回路２２０は、信号Ｓ１１を受け取ると、エラー訂正処理を行い、信号Ｓ１２＝Header（暗号鍵BE_i）｜Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）と、信号Ｓ１３＝Encryption（コンテンツ，コンテンツ暗号鍵AE_R）とを、コンテンツ復号鍵復号回路２４０、データ復号回路２５０にそれぞれ出力する（ステップＳＴ１２）。

【００７０】

コンテンツ復号鍵復号回路２４０は、信号Ｓ１２のHeader（暗号鍵BE_i）と、復号鍵記憶装置２３０に記憶されているＭ個の復号鍵BD_jのHeader（復号鍵BD_j）とを比較し、一致するものがあるか否かを調べる（ステップＳＴ１３）。

【００７１】

ここで、一致した場合（Ｙｅｓの場合）には、コンテンツ復号鍵復号回路２４０は、復号鍵記憶装置２３０に記憶されている復号鍵BD_jを用いて、コンテンツ復号鍵AD_Rを復号し、その鍵を信号Ｓ１５としてデータ復号回路２５０に出力する（ステップＳＴ１４）。

データ復号回路２５０は、信号Ｓ１５を受け取ると、そのコンテンツ復号鍵AD_Rを用いて、コンテンツを復号し、そのコンテンツを信号Ｓ１６としてデコーダ２６０に出力する（ステップＳＴ１５）。

【００７２】

デコーダ２６０は、信号Ｓ１６を受け取ると、そのコンテンツを再生（デコード）する（ステップＳＴ１６）。コンテンツの再生が完了すれば、再生装置２００での再生処理も終了する（ステップＳＴ１７）。

【００７３】

一方、ステップＳＴ１３において、一致するものがない場合（Ｎｏの場合）には、その光ディスク２０１は、その再生装置２００では再生が許可されていないことになるため、コンテンツを再生することなく処理を終了する（ステップＳＴ１７）。

【００７４】

[実施形態の効果]

本実施形態においては、コンテンツを再生が許可された地域の組み合わせ毎に異なるコンテンツ暗号鍵AE_Rで暗号化し、それを復号するためのコンテンツ復号鍵AD_Rをさらに複数の暗号鍵BE_iで暗号化しているので、再生を許可する再生装置のみが保有する復号鍵BD_jに対応する暗号鍵BE_iを用いてコンテンツ復号鍵AD_Rを暗号化して記録メディアに記録しておくことで、コンテンツを再生できる再生装置を制限することができる。

そして、この暗号鍵BE_iおよび復号鍵BD_jを、予め設定された地域毎に異なるように設定しているので、再生を許可する地域に設定された暗号鍵BE_iのみを用いることで、リージョンコードを用いずに、地域限定の再生制御を行うことができる。

さらに、暗号鍵BE_iを適宜設定することで、再生許可された地域にある再生装置であっても個別に再生を制限することもできる。

このため、リージョンコードのみによって再生制御を行っている従来の方式に比べて、コンテンツの著作権保護の観点からは、はるかに高い安全性を実現することができる。

【００７５】

また、再生が許可された地域毎やその地域の組み合わせ毎に異なるコンテンツ復号鍵AD_R、コンテンツ暗号鍵AE_Rを用い、かつ再生装置の保有する復号鍵BD_jや対応する暗号鍵BE_iを管理する部分木が再生地域ごとに独立しているため、ある特定の再生地域のコンテンツ復号鍵AD_Rや、その再生地域に属する再生装置の保有する復号鍵BD_jが漏洩しても、他の再生地域で再生を許可しているメディアや再生装置には何の影響も及ぼさない。このため、従来の文献１，２のように、再生地域ごとに分割されていない木構造を採用しており、かつコンテンツ暗号鍵、コンテンツ復号鍵も再生許可されている地域ごとに異なるものとしていない場合に比べても、鍵の漏洩対策を非常に簡単に行うことができる。

【００７６】

コンテンツ暗号鍵AE_Rと、暗号鍵BE_iという２種類の暗号鍵を用いることにより、コンテンツ復号鍵AD_Rの漏洩対策として再生装置側の復号鍵等の変更を全く必要としないで、コンテンツ復号鍵AD_Rを更新することができる。

従って、仮にコンテンツ復号鍵AD_Rが漏洩しても、新しいコンテンツ復号鍵AD_{2R}を用いて新たなメディアを作成するだけで対応でき、再生装置側の復号鍵BD_jは全く変更する必要がない。このため、再生装置側も変更する場合に比べて、コンテンツ復号鍵AD_Rの漏洩対策を簡単に行え、著作権保護の実効を図ることができる。

【００７７】

また、ある再生装置の復号鍵BD_jが漏洩した場合も、メディア側の記録を変更するだけで、対象再生地域のすべての再生装置に対して特定の再生装置の持つ復号鍵BD_jのみを無効化することができるので、再生装置側の変更を全く必要としないで再生可能とする復号鍵BD_jを更新することができる。

このように、ユーザー側にある再生装置の変更が不要であり、コンテンツ供給側のみで漏洩対策を行うことができるので、非常に効率的にかつ迅速にコンテンツの保護を図ることができる。

【００７８】

本実施形態では、リージョンコードを用いずに、木構造を改良した鍵管理方式

で地域限定再生制御を実現しているので、コピープロテクションのために木構造を用いた鍵管理方式を用いているシステムに対しては、本方式の地域限定再生制御を加える場合、メディア側および再生装置側のいずれにも余分に追加しなければならない装置が全く無く、極めて簡単にかつ低コストで導入することができる。

すなわち、木構造の鍵管理方式によるコピープロテクションシステムと、リージョンコード等のフラグによる地域限定再生制御を併用する場合には、メディア側には鍵情報の他にフラグを追加しなければならず、かつ再生装置側には鍵情報の処理手段の他に、フラグを識別し処理する手段を設けなければならない。これに対し、本実施形態では、メディア側には鍵情報のみを記録すればよく、フラグを追加する必要がなく、再生装置側にもフラグを処理する手段を設ける必要がないため、回路等の構成を簡易化できてコストも低減することができる。その上、従来のフラグを用いた場合と同様の地域限定再生制御を行えるとともに、鍵管理方式に応じたコピープロテクションシステムも実現でき、従来と同等以上の著作権保護機能を実現することができる。

【００７９】

予め設定された再生地域ごとに木構造を分割しているので、再生装置側が予め保有しておく復号鍵BD_jの数を減らすことができる。すなわち、図１、２に示す従来の鍵管理構造では、再生装置がＮ台ある場合、各再生装置は、$\log_2 N+1$の復号鍵を保有することになる。一方で、本実施形態では、再生地域がＲ個であれば、各再生装置が保有する復号鍵BD_jは、$\log_2(N/R)+1$に減少できる。従って、各再生装置２００における復号鍵記憶装置２３０の記憶容量も小さくすることができ、その分、コストも低減することができる。

【００８０】

再生を同時に許可する再生地域数によっては、メディアに記録しておく暗号化されたコンテンツ復号鍵AD_R＝Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）のデータ量の上限を従来に比べて減らすことができる。

すなわち、メディアに記録される暗号化されたコンテンツ復号鍵AD_R＝Encryption（コンテンツ復号鍵AD_R，暗号鍵BE_i）の数の上限は、図１，２に示すような

従来のComplete Subtree Method を用いた場合、無効化したい再生装置の数をｒ、再生装置の総数をＮとすると、$r\log_2(N/r)$で表される。本方式では、再生地域ごとに独立してComplete Subtree Method を用いていることになるため、同時に再生を許可したい再生地域が１つの場合には、再生装置数がＮからＮ／Ｒ（Ｒは再生地域の総数）に減少したものと見なすことができる。このため、メディアに記録されるコンテンツ復号鍵AD_Rの数の上限は、$r\log_2(N/(Rr))$となり、従来に比べて明らかに小さくすることができる。

【００８１】

一方、同時に再生を許可したい再生地域が複数存在する場合は、初期状態（対象再生地域において再生装置を無効化していない状態）において、対象再生地域のすべてのルートに割り当てられた暗号鍵BE_iでコンテンツ復号鍵AD_Rを暗号化し、メディアに記録しておかなければならない。この分のオーバーヘッドにより、各メディアに記録されるコンテンツ復号鍵AD_Rの数の上限は必ず減少する訳ではない。しかしながら、通常は、同時に再生を許可する再生地域数の増加によるオーバーヘッドに比べて、無効化したい再生装置数の増加によるオーバーヘッドのほうがはるかに多いため、通常の使用ではその増加は殆ど無視でき、実際にはコンテンツ復号鍵AD_Rを減少できる。

【００８２】

メディアに記録しておく暗号化されたコンテンツ復号鍵AD_Rのデータ量を一定とすると、無効化することができる再生装置の上限を増やすことができ、より多くの再生装置を無効化することができる。

【００８３】

メディアには、復号鍵用暗号鍵の種類を示すヘッダー情報も記憶しているので、各再生装置では、ヘッダー情報を参照することで、各再生装置が有する復号鍵用復号鍵で復号できるのかを容易にかつ迅速に判断でき、復号処理を高速化することができる。

【００８４】

［第２実施形態］

次に、本発明の第２実施形態について、図２２を参照して説明する。

第２実施形態は、第１実施形態とは、１つの地域に複数の木構造を設けている点のみが異なるものであり、記録装置１００や再生装置２００等、その他の構成は第１実施形態と同じであるため、それらの構成に関する説明は省略し、鍵管理方式のみ説明する。

【００８５】

本実施形態では、再生地域１には、２つの木構造が設けられている。各部分木のルートおよびリーフを含む各ノードには、前記第１実施形態と同様に、暗号鍵BE_iとそれに対応する復号鍵BD_jが一つずつ割り当てられている。そして、各再生装置は、自身が割り当てられたリーフから部分木のルートに至るパス上に存在する復号鍵BD_jを予め保有している。

なお、各暗号鍵BE_i、復号鍵BD_jは前記第１実施形態と同じく他の各ノードに割り当てられた各暗号鍵BE_i、復号鍵BD_jと異なるユニークな鍵であり、各暗号鍵BE_i同士や復号鍵BD_j同士で同一の鍵は存在しないように設定されている。従って、再生地域１の２つの木構造の各ノードに設定された鍵同士も互いに異なる鍵とされている。

このため、再生地域１における地域別暗号鍵、復号鍵は、再生地域１の２つの部分木のルートに割り当てられた暗号鍵BE_4，BE_5および復号鍵BD_4，BD_5の２種類の鍵を少なくとも含んでいる。従って、再生地域１用のメディア３０４には、各暗号鍵BE_4，BE_5で暗号化されたコンテンツ復号鍵AD_{R1}が記録されている。

【００８６】

この再生地域１における複数の木構造の割り当て方法は、例えば、各再生地域が現在のリージョンコードに対応する範囲で設定されている場合には、リージョンコード内の地域をより細かく設定したり、再生装置のメーカー毎に設定するなど、実施にあたって適宜設定すればよい。

なお、再生地域１においては、２つの部分木を設けていたが、３つ以上の部分木を設けてもよい。また、他の再生地域２～４においても、２つ以上の部分木を設けてもよい。要するに、各再生地域１～４には、１つ以上の部分木（木構造）が設定されて鍵が管理されていればよい。

【００８７】

〔第２実施形態の効果〕

このような第２実施形態においても、前記第１実施形態と同じ作用効果を奏することができる。

さらに、再生地域１のように、１つの再生地域において複数の木構造（部分木）を設定すれば、その再生地域内に設けられた再生装置の台数が多くなった場合でも、木構造の階層を少なくでき、鍵管理を容易に行うことができる。特に、１つの再生地域１内に、より狭い地域、例えば、国毎、都道府県毎などで部分木を分けたり、再生装置のメーカー毎に分けるなどすることで、鍵管理を行いやすくできるため、使い勝手のよい鍵管理方式を提供することができる。

【００８８】

［第３実施形態］

次に、本発明の第３実施形態について、図２３～２５を参照して説明する。

第３実施形態は、第１実施形態とは、鍵管理方式が異なるものであり、記録装置１００等のその他の構成は第１実施形態と同じであるため、その構成に関する説明は省略し、鍵管理方式のみ説明する。

【００８９】

本実施形態の鍵管理方式は、前記文献２の木構造パターン分割方式を応用したものである。木構造パターン分割方式は、前記文献２に記載されているように、木構造におけるノードの位置する各層（レイヤ）の各ノードに、そのノードの１層下のレイヤのノードの無効化パターン毎に鍵を割り当てたものである。

すなわち、図２３，２４に示すように、各再生地域のルート（レイヤ０）には、その下位レイヤ（レイヤ１）の各ノード（ノード０～３）を無効化するパターンに対応する各鍵「$_{0\text{-}0}K_{0000}$～$_{0\text{-}0}K_{1110}$」が設定されている。なお、図２４に示すように「Ｋ」の左側の数字は、「レイヤ番号－相対ノード番号」を示し、右側の４桁の数字は「ノード無効化パターン」を示す。ノード無効化パターンは、各桁が各ノード０～３に対応しており、無効化するノードに対応する桁は「１」で示されている。本実施形態では、４分木の木構造を用いているので、ノード無効化パターンも４桁（４ビット）であるが、３分木の木構造であれば３桁（３ビット）で表される。なお、「$_{0\text{-}0}K_{1111}$」はすべてのノードを無効化した場合を表す

が、この場合は再生させるための鍵を設定する必要はないため、その鍵は設けられていない。

【００９０】

この無効化パターンに対応して異なる鍵を割り当てる考え方を、各レイヤのノード毎に再帰的に適用することで、各無効化パターンに対応する鍵が割り当てられている。なお、レイヤ１以下では、すべてのノードを有効化する鍵は「$_{1\text{-}0}K_{0000}$」等で表されるが、このような鍵は、その上のレイヤにおいてレイヤ１のノードを有効化すればよいため、設けられていない。また、すべてのノードを無効化する鍵もルートの場合と同じ理由で設けられていない。

【００９１】

そして、各再生装置は、自らが有効とされている、つまり無効化されていないパターンに対応する鍵を所有している。例えば、図２４において、再生装置４は、レイヤ０の鍵のうち、自らが所属するレイヤ１のノード０が有効化されている鍵「$_{0\text{-}0}K_{0}$***」つまり４桁のパターン部分で最も左側の桁（レイヤ１のノード０に対応する桁）が有効を示す「０」である８個の鍵（図２４では黒枠で囲まれた鍵）と、レイヤ１のノード０に設定された鍵のうち、再生装置４が有効化されている鍵「$_{1\text{-}0}K$***$_{0}$」つまり４桁のパターン部分で最も右側の桁が「０」である７個の鍵（同じく黒枠で囲まれた鍵）を所有している。

【００９２】

このように設定された木構造パターン分割方式では、再生装置を無効化するには、その再生装置を無効化するパターンの鍵を選択し、その鍵を利用してコンテンツ復号鍵を暗号化すればよい。例えば、図２５に示すように、再生装置４，７を無効化する場合、レイヤ０からは再生装置９～１６のみを有効化するパターンに対応する鍵「$_{0\text{-}0}K_{1100}$」を選択し、レイヤ１では、ノード０，１において、再生装置４，７のみを無効化するパターンに対応する鍵「$_{1\text{-}0}K_{0001}$」、「$_{1\text{-}1}K_{0010}$」を選択する。

これらの鍵でコンテンツ復号鍵ADを暗号化してメディアに記録すれば、再生装置９～１６は、鍵「$_{0\text{-}0}K_{1100}$」に対応する復号鍵BDを備えているので、その鍵BDを用いてコンテンツ復号鍵ADを復号し、コンテンツを復号できる。また、再生装

置１～３，５，６，８は、この鍵「$_{0-0}K_{1100}$」では無効化されているためコンテンツを復号できないが、鍵「$_{1-0}K_{0001}$」、「$_{1-1}K_{0010}$」に対応する復号鍵BDを備えているので、それらの鍵BDを用いてコンテンツ復号鍵ADを復号し、コンテンツを復号できる。

【００９３】

本実施形態では、図２３に示すように、このような木構造（部分木）を各再生地域ごとに独立して設けており、各パターンに対応する鍵はユニークな鍵とされている。従って、いずれかの鍵に基づいて再生地域も特定できるため、これらの各鍵は地域別暗号鍵、復号鍵としても機能する。

なお、第２実施形態と同様に、各再生地域には２つ以上の木構造（部分木）を設定してもよい。

【００９４】

［第３実施形態の効果］

このような第３実施形態においても、再生が許可された地域毎やその地域の組み合わせ毎に異なるコンテンツ復号鍵AD、コンテンツ暗号鍵AEを用い、かつ再生装置の保有する復号鍵や対応する暗号鍵を管理する部分木が再生地域ごとに独立しているため、ある特定の再生地域のコンテンツ復号鍵ADや、その再生地域に属する再生装置の保有する復号鍵が漏洩しても、他の再生地域で再生を許可しているメディアや再生装置には何の影響も及ぼさないようにできるなど、前記第１，２実施形態と同様の作用効果を奏することができる。

【００９５】

さらに、鍵管理方式に木構造パターン分割方式を採用したので、再生装置を無効化する際に、メディア側に記録する鍵の量を前記各実施形態に比べて少なくすることができる。すなわち、無効化する場合には、無効化される再生装置からルートに至る各ノードにおいては、対応するパターンに応じた１つの鍵を選択すればよいため、無効化する再生装置が増えても、メディアに記録する鍵の数の増加を抑えることができる。従って、メディアにおける鍵を記録する領域を小さくでき、その分、コンテンツの記録量を大きくすることができる。

【００９６】

［第４実施形態］

次に、本発明の第４実施形態について、図２６を参照して説明する。

前記各実施形態では、コンテンツデータをコンテンツ暗号鍵で直接暗号化し、この暗号化されたデータをコンテンツ復号鍵で直接復号していたが、第４実施形態の記録再生システムでは、コンテンツデータをコンテンツ暗号鍵を用いて間接的に暗号化し、この暗号化されたデータをコンテンツ復号鍵を用いて間接的に復号したものである。

【００９７】

本実施形態では、記録装置５００は、コンテンツＳ３１のタイトル毎に設定されるタイトル鍵Ｓ３２を設定して出力するタイトル鍵設定回路５１０と、一方向性関数回路５２０と、コンテンツ暗号回路５３０とを備える。一方向性関数回路５２０は、コンテンツＳ３１の一部のデータＳ３３と前記タイトル鍵Ｓ３２とが入力され、所定の値（データ）Ｓ３４を出力する。なお、一方向性関数回路５２０では、出力値から入力値は容易に求めることができない一方向関数を用いた回路である。

そして、コンテンツ暗号回路５３０は、前記一方向性関数回路５２０から出力された値（データ）Ｓ３４を暗号鍵とし、コンテンツＳ３１を暗号化し、コンテンツ暗号データＳ３５を出力する。

【００９８】

また、鍵管理センター６００は、コンテンツ鍵入力回路６１０と、タイトル鍵暗号化回路６２０と、復号鍵用暗号鍵入力回路６３０と、コンテンツ鍵暗号化回路６４０とを備える。

タイトル鍵暗号化回路６２０は、コンテンツ再生地域に応じてコンテンツ鍵入力回路６１０で入力されたコンテンツ鍵（コンテンツ暗号鍵）Ｓ４１を用い、前記タイトル鍵Ｓ３２を暗号化し、タイトル鍵暗号化データＳ４２を出力する。

さらに、鍵管理センター６００のコンテンツ鍵暗号化回路６４０は、鍵管理センター６００の復号鍵用暗号鍵入力回路６３０でコンテンツの再生地域および再生が許可されている再生装置に応じて入力された復号鍵用暗号鍵Ｓ４３を用い、前記コンテンツ鍵（ここではコンテンツ復号鍵として機能する）Ｓ４１を暗号化

し、コンテンツ鍵暗号データＳ４４を出力する。

そして、コンテンツ暗号データＳ３５、コンテンツの一部データであるタイトル鍵変換データＳ３３、タイトル鍵暗号データＳ４２、コンテンツ鍵暗号データＳ４４は、光ディスク５０１やその原盤に記録される。

【００９９】

一方、再生装置７００は、復号鍵記憶装置７１０、コンテンツ鍵復号回路７２０、タイトル鍵復号回路７３０、一方向性関数回路７４０、コンテンツ復号回路７５０を備えている。

復号鍵記憶装置７１０は、その再生装置７００に対応する復号鍵用復号鍵Ｓ５１を記憶している。そして、光ディスク５０１を読み込むと、コンテンツ鍵復号回路７２０は、読み込んだコンテンツ鍵暗号データＳ４４を前記復号鍵用復号鍵Ｓ５１を用いて復号する。この際、前記復号鍵用暗号鍵Ｓ４３が再生を許可している再生装置７００であれば、コンテンツ鍵復号回路７２０での復号に成功するが、許可されていない再生装置７００では、前記復号鍵用暗号鍵Ｓ４３に対応する復号鍵用復号鍵Ｓ５１を備えていないため、その復号に失敗し、コンテンツも復号することができない。

【０１００】

コンテンツ鍵復号回路７２０は、復号に成功するとコンテンツ鍵データＳ５２を出力する。このコンテンツ鍵データＳ５２は、タイトル鍵復号回路７３０で復号鍵として用いられ、タイトル鍵Ｓ５３が復号される。

この復号されたタイトル鍵Ｓ５３と、タイトル鍵転換データＳ３３とは、前記一方向性関数回路５２０と同一の一方向性関数回路７４０に入力され、前記値Ｓ３４と同じ値Ｓ５４が出力される。

そして、コンテンツ復号回路７５０では、この値Ｓ５４を用いてコンテンツ暗号データＳ３５を復号し、コンテンツを出力する。

【０１０１】

[第４実施形態の効果]

このような本実施形態によれば、コンテンツ暗号鍵で直接コンテンツを暗号化せずに、タイトル鍵や一方向性関数回路５２０を介して間接的に暗号化している

ため、タイトル鍵を変更することで容易にコンテンツ暗号データも変更でき、より著作権保護機能を強化することができる。特に、再生地域別に設定されるコンテンツ鍵を変更しなくても、タイトル鍵のみを変更することでコンテンツ暗号データを異なるものにできるため、コンテンツの種類毎にタイトル鍵を変更することなども頻繁に行うことができ、著作権保護機能をより一層強化できる。

【０１０２】

なお、鍵管理センター６００は、独立した組織として設けられていてもよいが、記録装置５００側つまりコンテンツを有する著作権者や光ディスク５０１を製造する製造会社等に組み込まれていてもよい。

【０１０３】

〔実施形態の変形〕

なお、本発明は、上述した実施形態に限定されるものではなく、本発明の目的を達成できる範囲で以下に示される変形をも含むものである。

【０１０４】

例えば、復号鍵用暗号鍵および復号鍵用復号鍵の鍵管理方式としては、前記第１，２実施形態に示す鍵管理方式や前記第３実施形態に示す木構造パターン分割方式に限らず、例えば、上記文献１に記載された「The Subset Difference Method」等の他の鍵管理方式を用いてもよい。

また、鍵管理方式としては、必ずしも木構造を利用した鍵管理方式に限らず、他の方式を用いてもよい。例えば、各再生装置に設定された復号鍵用暗号鍵、復号鍵と、それらの各再生装置が属する再生地域との対応情報を予め用意しておき、再生許可された地域に所属する各再生装置の復号鍵用暗号鍵を用いて各コンテンツ復号鍵を暗号化するなど、他の鍵管理方式を用いてもよい。要するに、コンテンツ復号鍵を暗号化する復号鍵用暗号鍵およびそれに対応する復号鍵用復号鍵のペアが、少なくとも予め設定された地域毎に異なるものであればよい。

要するに、各再生装置を無効化するために、各再生装置に対応して設けられる復号鍵用暗号鍵および復号鍵用復号鍵の管理方式は、実施にあたって適宜選択することができ、少なくとも再生地域毎に異なる鍵として管理できるものであればよい。

但し、前記木構造を用いれば、無効化される再生装置の数に応じて使用する鍵の数も調整でき、特に無効化される再生装置が少ない初期段階では、使用する鍵の数を非常に少なくできるなど、鍵管理を容易に行うことができる。

【０１０５】

また、記録装置１００，５００や再生装置２００，７００の構成は、前記各実施形態のものに限らない。要するに、記録装置は、コンテンツデータをコンテンツ暗号鍵を直接または間接的に利用して暗号化できればよく、再生装置はこの暗号化されたデータをコンテンツ復号鍵を直接または間接的に利用して復号化できるものであればよい。

要するに、本発明において、コンテンツ暗号鍵を利用してコンテンツを暗号化するとは、コンテンツ鍵を直接的または間接的に利用してコンテンツを暗号化することを意味する。同様に、前記暗号化されたコンテンツを復号化するために利用されるコンテンツ復号鍵とは、コンテンツに直接的または間接的に適用してコンテンツを復号化できるものを意味する。

【０１０６】

また、前記実施形態では、コンテンツ暗号鍵およびコンテンツ復号鍵は、コンテンツの再生が許可された地域毎あるいはその再生が許可されている地域の組み合わせ毎に設定され、かつ新しく無効化する再生装置が生じた場合には、新たな鍵に更新していたが、再生許可地域に属し、かつ再生が許可されている再生装置の組み合わせに対応して設定してもよい。この場合も、各再生装置自体が再生地域毎に分かれているため、コンテンツ暗号鍵およびコンテンツ復号鍵は、少なくとも再生地域毎あるいはその組み合わせ毎に異なる鍵となる。このような場合は、図２０のフローチャートとは異なり、再生地域および再生装置を指定後に、各コンテンツ暗号鍵、コンテンツ復号鍵および復号鍵暗号鍵が設定されることになる。

【０１０７】

また、暗号化されたコンテンツやコンテンツ復号鍵を記録する記録メディアとしては、光ディスクに限らず、磁気ディスク、磁気テープ、メモリカード等の各種記憶メディアを利用してもよい。なお、記録装置１００のメディア記録手段１

８０や、再生装置２００の情報読取手段２１０は、利用する記録メディアの種類に応じて適宜設定すればよい。

【０１０８】

さらに、暗号化されたコンテンツやコンテンツ復号鍵は、情報配信装置であるコンテンツ配信用サーバに組み込まれた磁気ディスク等の記録メディアに記録されているものでもよい。このコンテンツ配信サーバに、記録メディアに記録された暗号化されたコンテンツ、コンテンツ復号鍵を配信する配信手段を設けることで、インターネットやＬＡＮなどを介してアクセスしてきた各再生装置２００に対し、前記コンテンツおよびコンテンツ復号鍵の暗号化データを送信することができる。そして、各再生装置２００は、この暗号化データを受信し、復号化して再生すればよい。

【０１０９】

コンテンツ暗号鍵AE_R、コンテンツ復号鍵AD_Rは、再生が許可された再生地域毎やその組合せに応じて設定され、メディア３０１，３０３のように、同じ再生地域内で無効化する再生装置が生じて、再生許可する再生装置の組合せが異なる場合に、異なる鍵を用いるようにしていたが、許可された再生地域の組合せが同じであり、かつ再生許可する再生装置の組合せが同じ場合でも異なる鍵を用いてもよい。

【０１１０】

配信されるコンテンツの種類としては、音楽データに限らず、映像やニュース等の文字情報などでもよく、顧客ニーズに応じて適宜設定すればよい。これらのコンテンツの種類は、コンテンツ配信事業を行う際に適宜設定すればよい。

【０１１１】

記録装置１００としては、各種ハードウェアを組み合わせた専用機に限らず、コンピュータのような汎用機に情報記録プログラムを組み込んで構成してもよい。特に、ＤＶＤ－Ｒ等の書き込み可能なドライブを有するコンピュータに前記情報記録プログラムを組み込むことで記録装置１００を構成すれば、少量の情報記録媒体を低コストで生産することができる。

【０１１２】

再生装置２００としては、ＤＶＤ再生機のような再生専用機に限らず、コンピュータのような汎用機に情報再生プログラムを組み込んで構成してもよい。

すなわち、再生装置２００としては、例えば、無線や有線等の各種通信機能を有する携帯電話機、ＰＤＡ（携帯情報端末）、オーディオ機器、車等に設けられるカーオーディオ機器等の各種の専用機やＰＣに代表される汎用機を利用できる。

なお、各プログラムを用いて記録装置１００や再生装置２００を構成するには、インターネット等の通信手段や、ＣＤ－ＲＯＭ、メモリカード等の記録媒体を介してプログラムをコンピュータ等にインストールし、このインストールされたプログラムでＣＰＵ等を動作させて実現させればよい。

【０１１３】

コンテンツ再生の許可・不許可を制御するための再生地域としては、通常は、市町村、県、国、大陸別等の地理的に設定される区域によって区分けされるが、例えば、特定のメーカーの再生装置のみで再生可能に制御する場合のように、地理的以外の区分けで設定してもよい。

【０１１４】

その他、本発明の実施の際の具体的な構造などは、本発明の目的を達成できる範囲で他の構造や手順でもよい。

【図面の簡単な説明】

【図１】

本発明の従来技術における鍵管理方式を示す模式図である。

【図２】

本発明の従来技術における鍵管理方式を示す模式図である。

【図３】

本発明の実施形態における記録装置の構成を示すブロック図である。

【図４】

図３における信号Ｓ１のデータフォーマットを示す図である。

【図５】

図３における信号Ｓ２のデータフォーマットを示す図である。

【図６】

図３における信号Ｓ３のデータフォーマットを示す図である。

【図７】

図３における信号Ｓ４のデータフォーマットを示す図である。

【図８】

図３における信号Ｓ５のデータフォーマットを示す図である。

【図９】

図３における信号Ｓ６のデータフォーマットを示す図である。

【図１０】

図３における信号Ｓ７のデータフォーマットを示す図である。

【図１１】

前記実施形態における再生装置の構成を示すブロック図である。

【図１２】

図１１における信号Ｓ１１のデータフォーマットを示す図である。

【図１３】

図１１における信号Ｓ１２のデータフォーマットを示す図である。

【図１４】

図１１における信号Ｓ１３のデータフォーマットを示す図である。

【図１５】

図１１における信号Ｓ１４のデータフォーマットを示す図である。

【図１６】

図１１における信号Ｓ１５のデータフォーマットを示す図である。

【図１７】

図１１における信号Ｓ１６のデータフォーマットを示す図である。

【図１８】

前記実施形態における鍵管理方式を示す模式図である。

【図１９】

前記実施形態における鍵管理方式を示す模式図である。

【図２０】

前記実施形態の記録装置の処理手順を示すフローチャートである。

【図２１】

前記実施形態の再生装置の処理手順を示すフローチャートである。

【図２２】

本発明の第２実施形態における鍵管理方式を示す模式図である。

【図２３】

本発明の第３実施形態における鍵管理方式を示す模式図である。

【図２４】

第３実施形態における鍵管理方式を示す模式図である。

【図２５】

第３実施形態における鍵管理方式を示す模式図である。

【図２６】

本発明の第４実施形態における記録再生システムの構成を示すブロック図である。

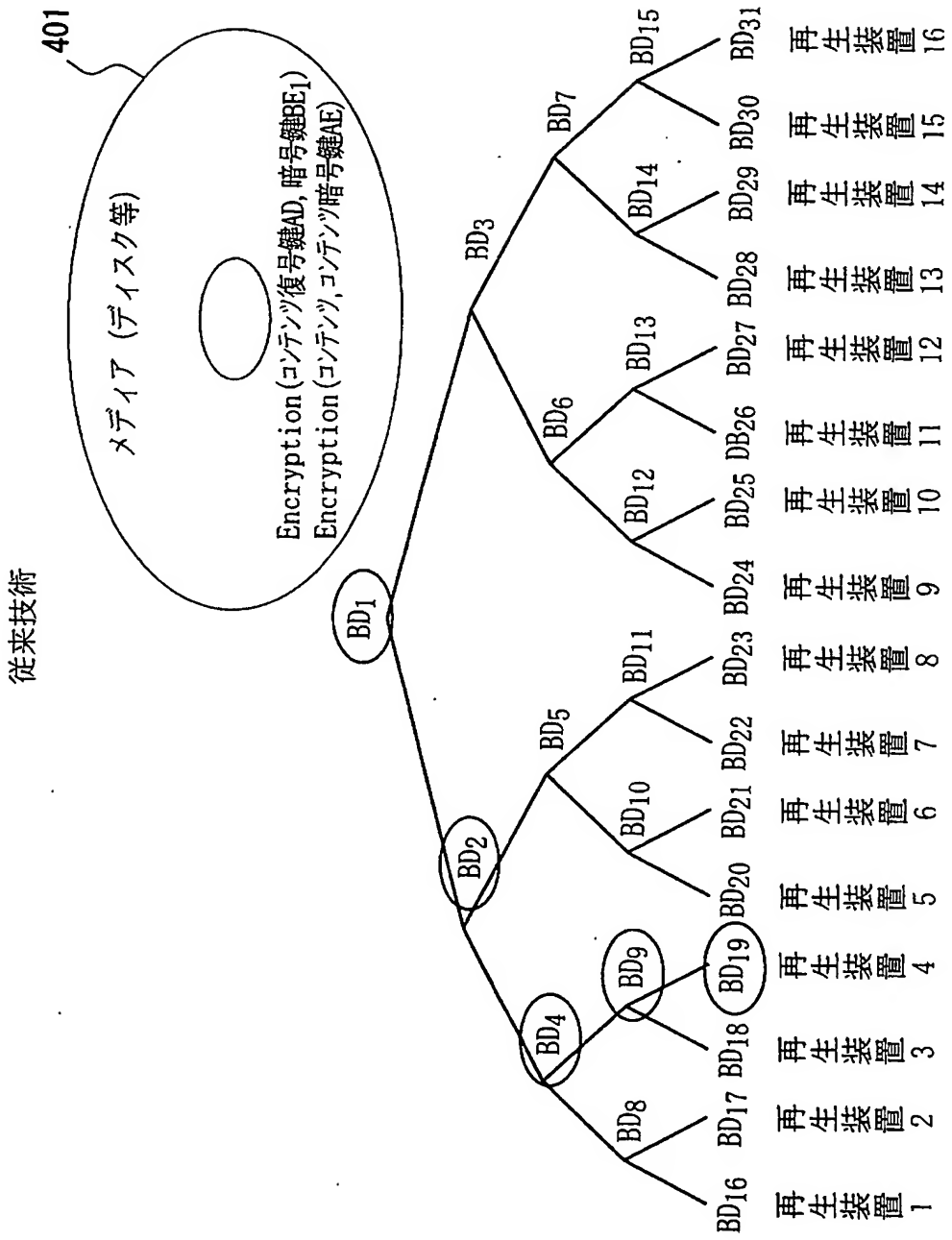
【符号の説明】

１００，５００　　記録装置
１０１　　原盤
１１０　　データ入力回路
１２０　　コンテンツ復号鍵入力回路
１３０　　コンテンツ暗号鍵入力回路
１４０　　データ暗号化回路
１５０　　鍵暗号鍵入力回路
１６０　　コンテンツ復号鍵暗号化回路
１７０　　エラー訂正回路
１８０　　メディア記録手段
２００，７００　　再生装置
２０１　　光ディスク
２１０　　情報読取手段
２２０　　エラー訂正回路

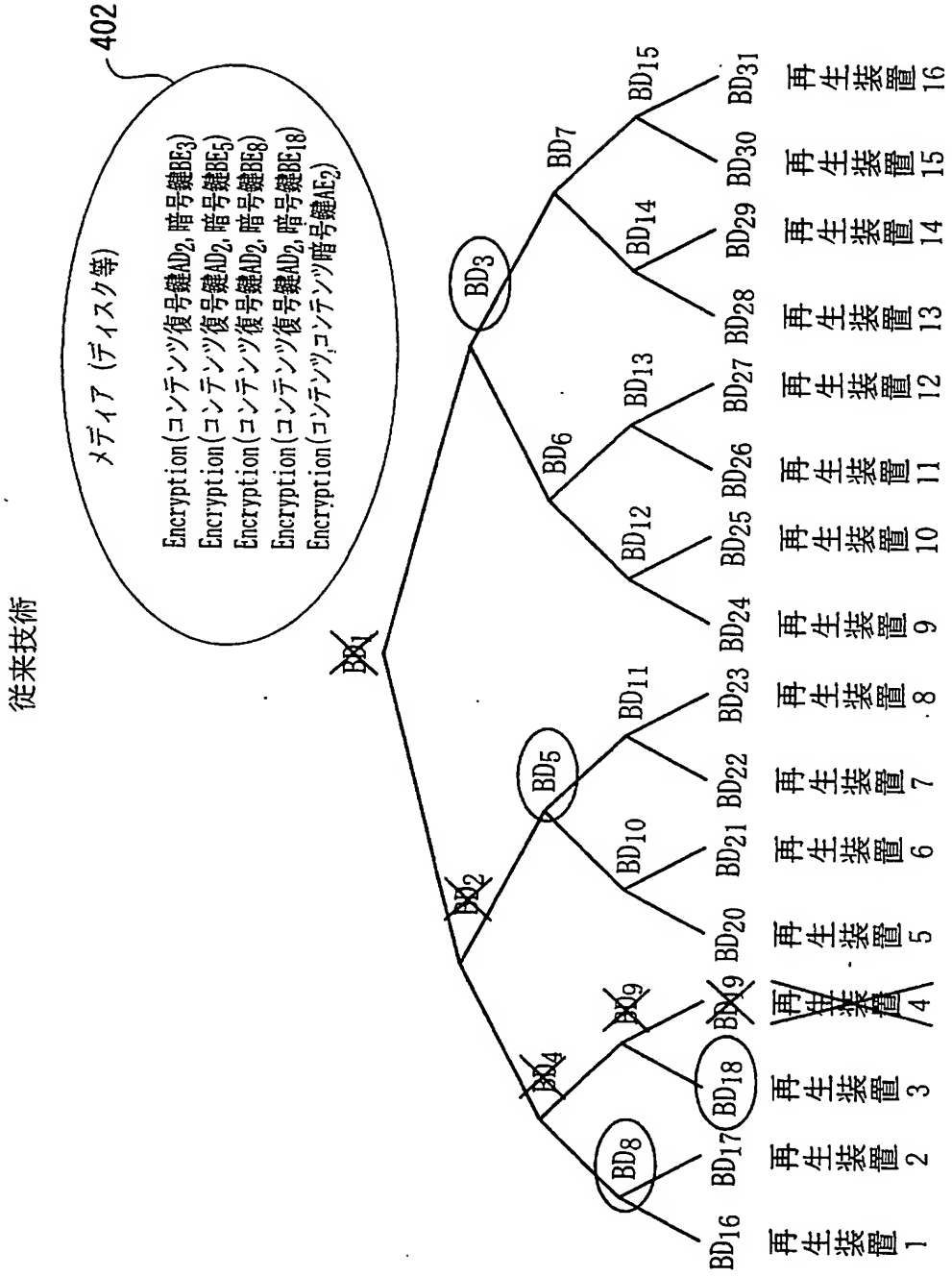
２３０　　復号鍵記憶装置
２４０　　コンテンツ復号鍵復号回路
２５０　　データ復号回路
２６０　　デコーダ
５３０　　コンテンツ暗号回路
６００　　鍵管理センター
６１０　　コンテンツ鍵入力回路
６３０　　復号鍵用暗号鍵入力回路
６４０　　コンテンツ鍵暗号化回路
７２０　　コンテンツ鍵復号回路
７５０　　コンテンツ復号回路

【書類名】　図面

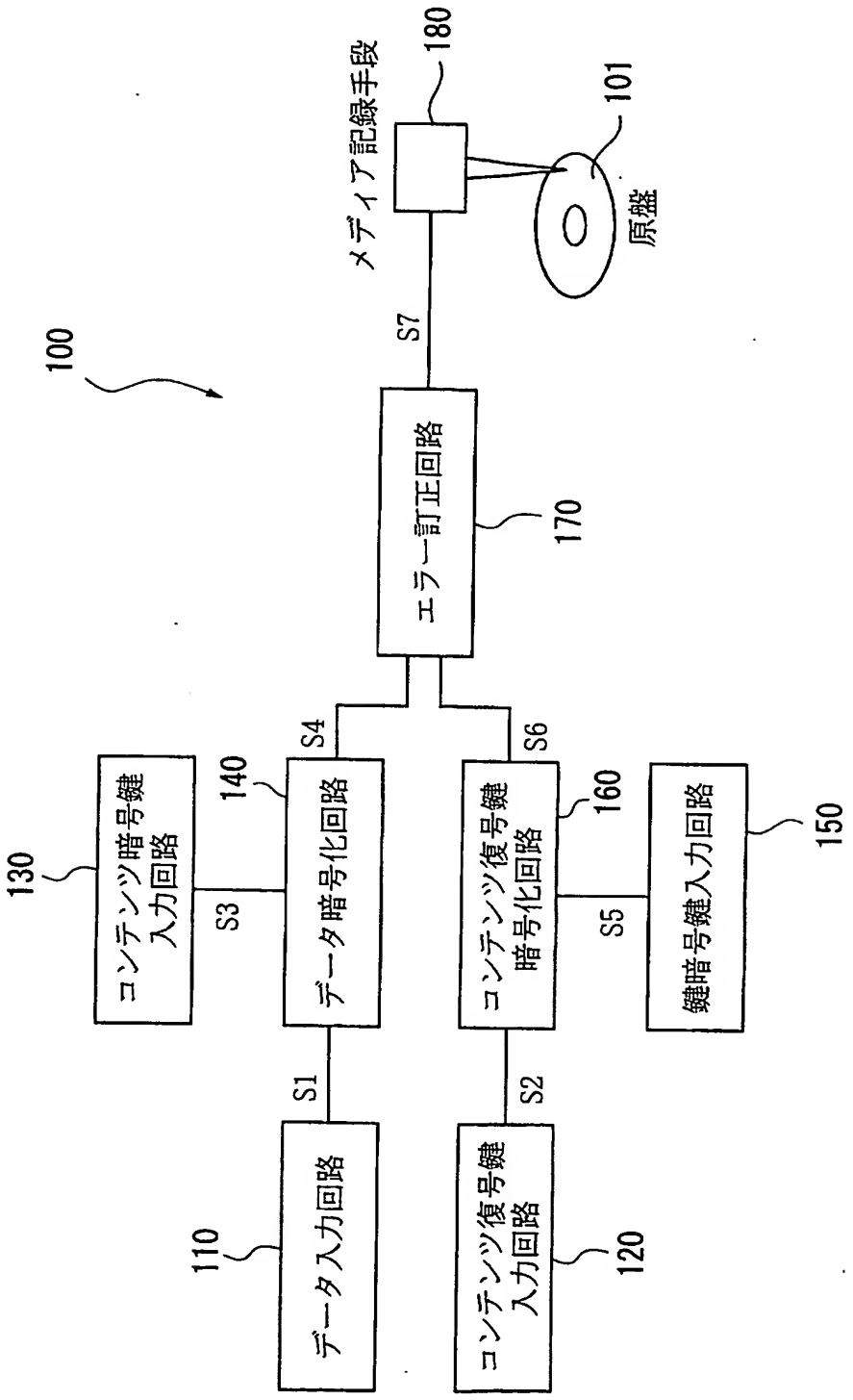
【図１】


401
メディア（ディスク等）
Encryption(ｺﾝﾃﾝﾂ復号鍵AD, 暗号鍵BE1)
Encryption(ｺﾝﾃﾝﾂ,ｺﾝﾃﾝﾂ暗号鍵AE)
従来技術
BD1
BD2
BD3
BD4
BD5
BD6
BD7
BD8
BD9
BD10
BD11
BD12
BD13
BD14
BD15
BD16
BD17
BD18
BD19
BD20
BD21
BD22
BD23
BD24
DB26
BD25
BD27
BD28
BD29
BD30
BD31
再生装置 1
再生装置 2
再生装置 3
再生装置 4
再生装置 5
再生装置 6
再生装置 7
再生装置 8
再生装置 9
再生装置 10
再生装置 11
再生装置 12
再生装置 13
再生装置 14
再生装置 15
再生装置 16

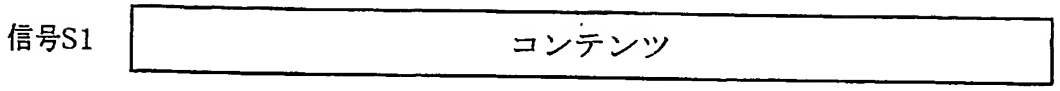
【図２】


従来技術
402
メディア（ディスク等）
Encryption(コンテンツ復号鍵AD2, 暗号鍵BE3)
Encryption(コンテンツ復号鍵AD2, 暗号鍵BE5)
Encryption(コンテンツ復号鍵AD2, 暗号鍵BE8)
Encryption(コンテンツ復号鍵AD2, 暗号鍵BE18)
Encryption(コンテンツ,コンテンツ暗号鍵AE2)
BD1
BD2
BD3
BD4
BD5
BD6
BD7
BD8
BD9
BD10
BD11
BD12
BD13
BD14
BD15
BD16
BD17
BD18
BD19
BD20
BD21
BD22
BD23
BD24
BD25
BD26
BD27
BD28
BD29
BD30
BD31
再生装置 1
再生装置 2
再生装置 3
再生装置 4
再生装置 5
再生装置 6
再生装置 7
再生装置 8
再生装置 9
再生装置 10
再生装置 11
再生装置 12
再生装置 13
再生装置 14
再生装置 15
再生装置 16

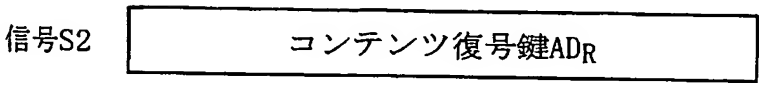
【図３】


100
メディア記録手段
180
101
原盤
S7
エラー訂正回路
170
S4
S6
コンテンツ暗号鍵
入力回路
130
140
データ暗号化回路
S3
コンテンツ復号鍵
暗号化回路
160
S5
鍵暗号鍵入力回路
150
S1
S2
データ入力回路
110
コンテンツ復号鍵
入力回路
120

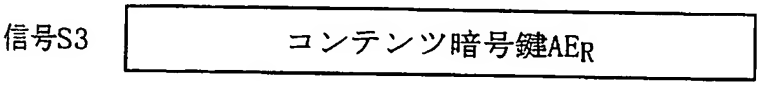
【図４】


信号S1
コンテンツ

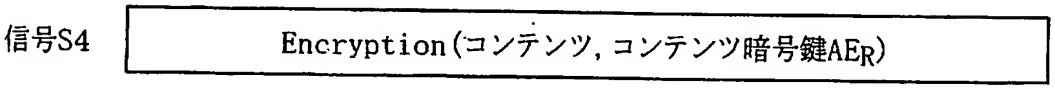
【図５】


信号S2
コンテンツ復号鍵AD_R

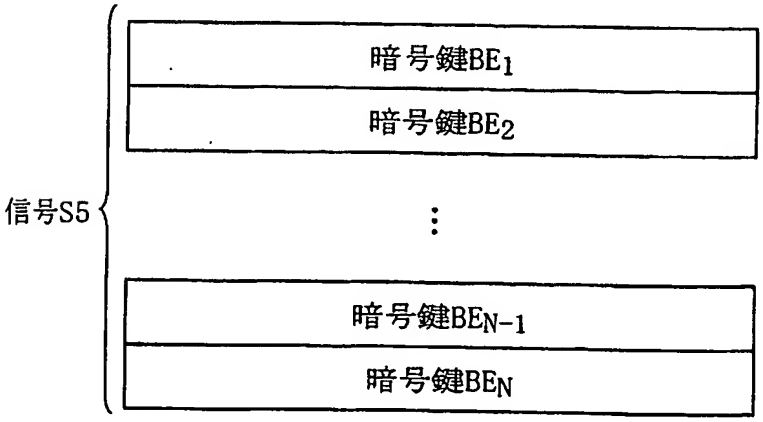
【図６】


信号S3
コンテンツ暗号鍵AE_R

【図７】


信号S4
Encryption(コンテンツ, コンテンツ暗号鍵AE_R)

【図８】


信号S5
暗号鍵BE_1
暗号鍵BE_2
暗号鍵BE_{N-1}
暗号鍵BE_N

【図９】

信号S6

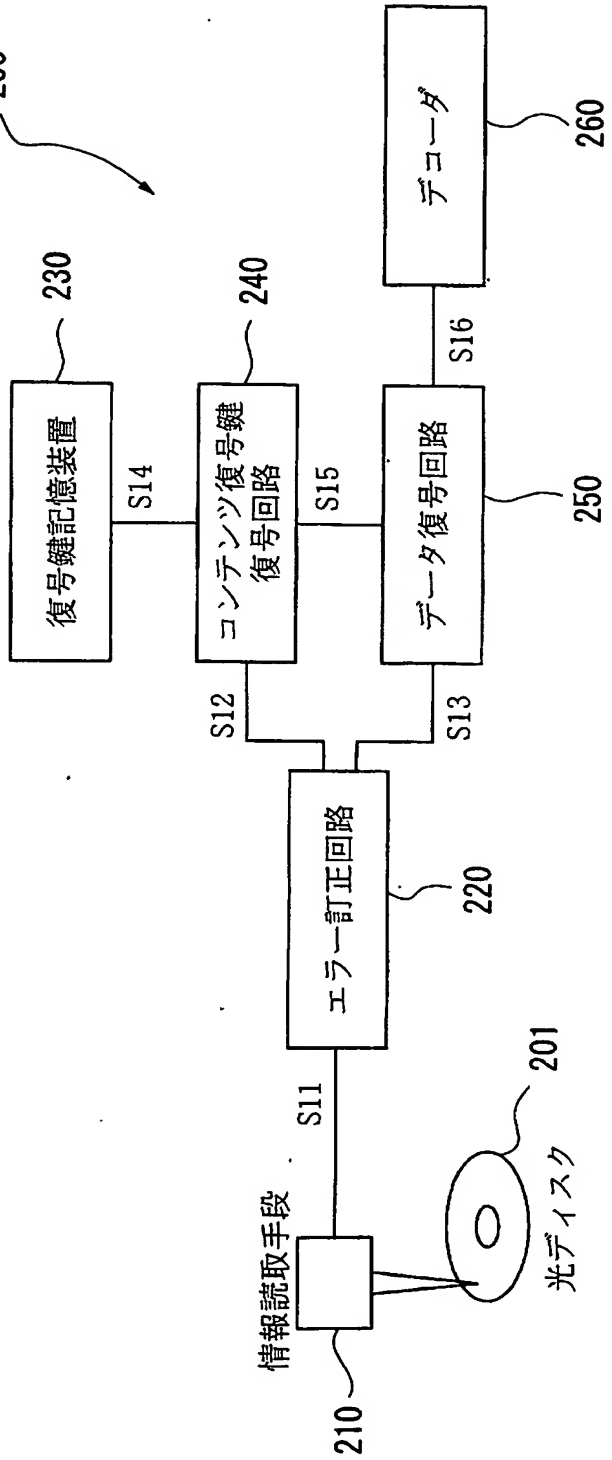
Header(暗号鍵BE_1)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_1)
Header(暗号鍵BE_2)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_2)
⋮	
Header(暗号鍵BE_{N-1})	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_{N-1})
Header(暗号鍵BE_N)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_N)

【図１０】

信号S7

Header(暗号鍵BE_1)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_1)
Header(暗号鍵BE_2)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_2)
⋮	
Header(暗号鍵BE_{N-1})	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_{N-1})
Header(暗号鍵BE_N)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_N)
Encryption(コンテンツ, コンテンツ暗号鍵AE_R)	
Error Correcting Code	

【図１１】


200
230
240
260
復号鍵記憶装置
S14
コンテンツ復号鍵
復号回路
S15
データ復号回路
250
S16
デコーダ
S12
S13
エラー訂正回路
220
S11
201
情報読取手段
光ディスク
210

【図１２】

信号S11

Header(暗号鍵BE_1)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_1)
Header(暗号鍵BE_2)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_2)
⋮	
Header(暗号鍵BE_{N-1})	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_{N-1})
Header(暗号鍵BE_N)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_N)
Encryption(コンテンツ, コンテンツ暗号鍵AE_R)	
Error Correcting Code	

【図１３】

信号S12

Header(暗号鍵BE_1)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_1)
Header(暗号鍵BE_2)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_2)
⋮	
Header(暗号鍵BE_{N-1})	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_{N-1})
Header(暗号鍵BE_N)	Encryption(コンテンツ復号鍵AD_R, 暗号鍵BE_N)

【図１４】

信号S13

Encryption(コンテンツ, コンテンツ暗号鍵AE_R)

【図１５】

信号S14

Header(復号鍵BD_1)	復号鍵BD_1
Header(復号鍵BD_2)	復号鍵BD_2
⋮	
Header(復号鍵BD_{M-1})	復号鍵BD_{M-1}
Header(復号鍵BD_M)	復号鍵BD_M

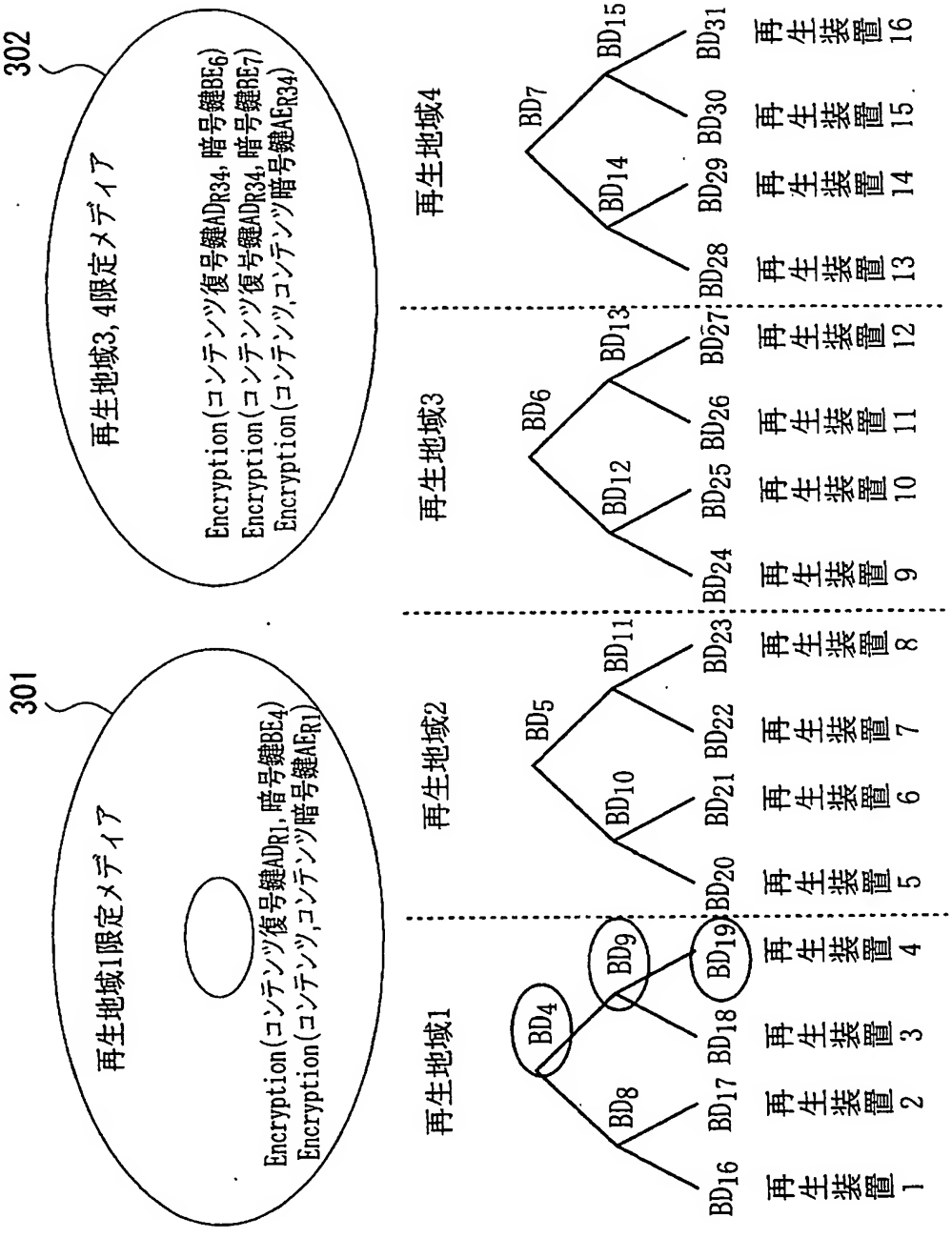
【図１６】

信号S15	コンテンツ復号鍵AD_R

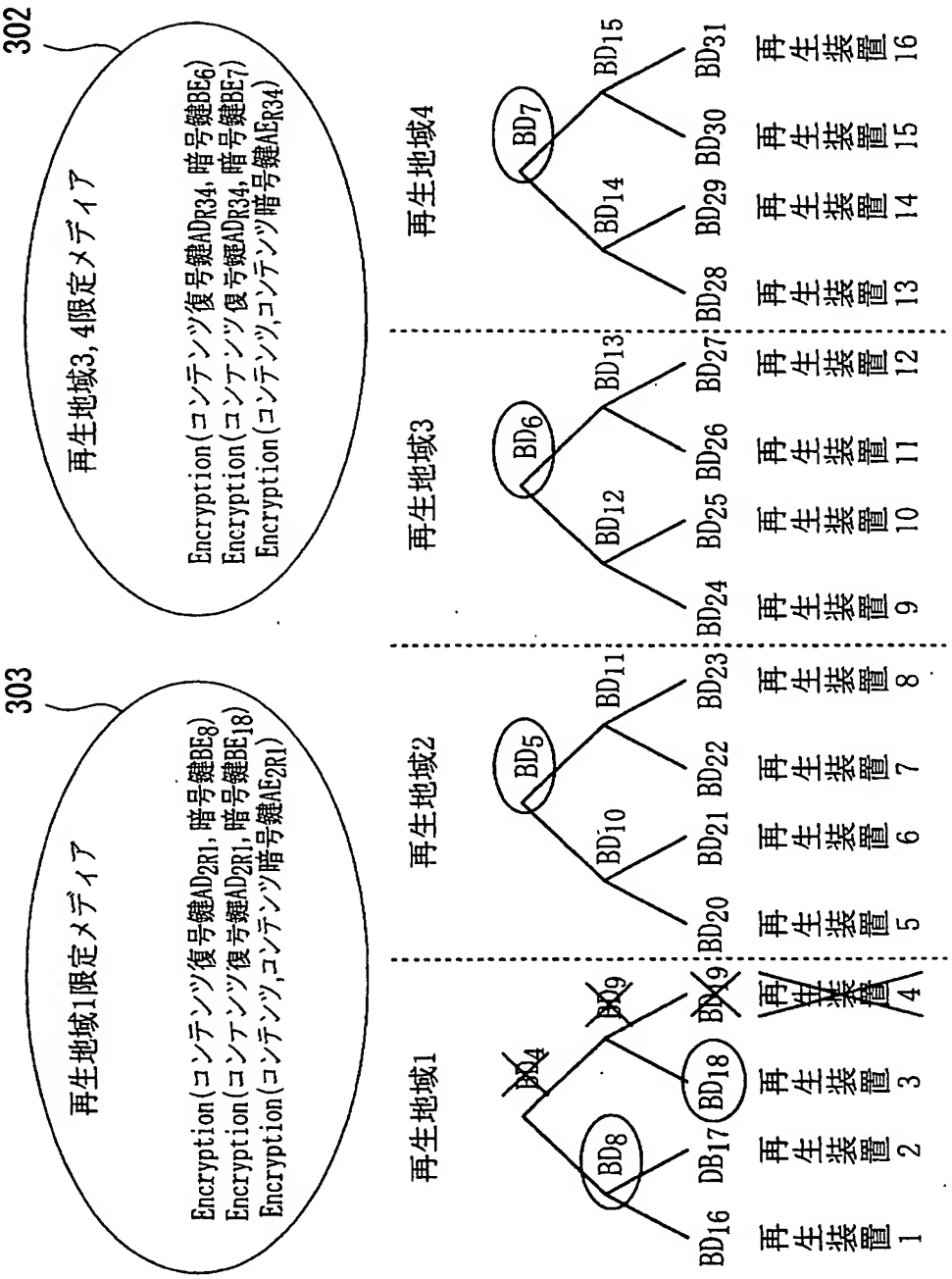
【図１７】

信号S16	コンテンツ

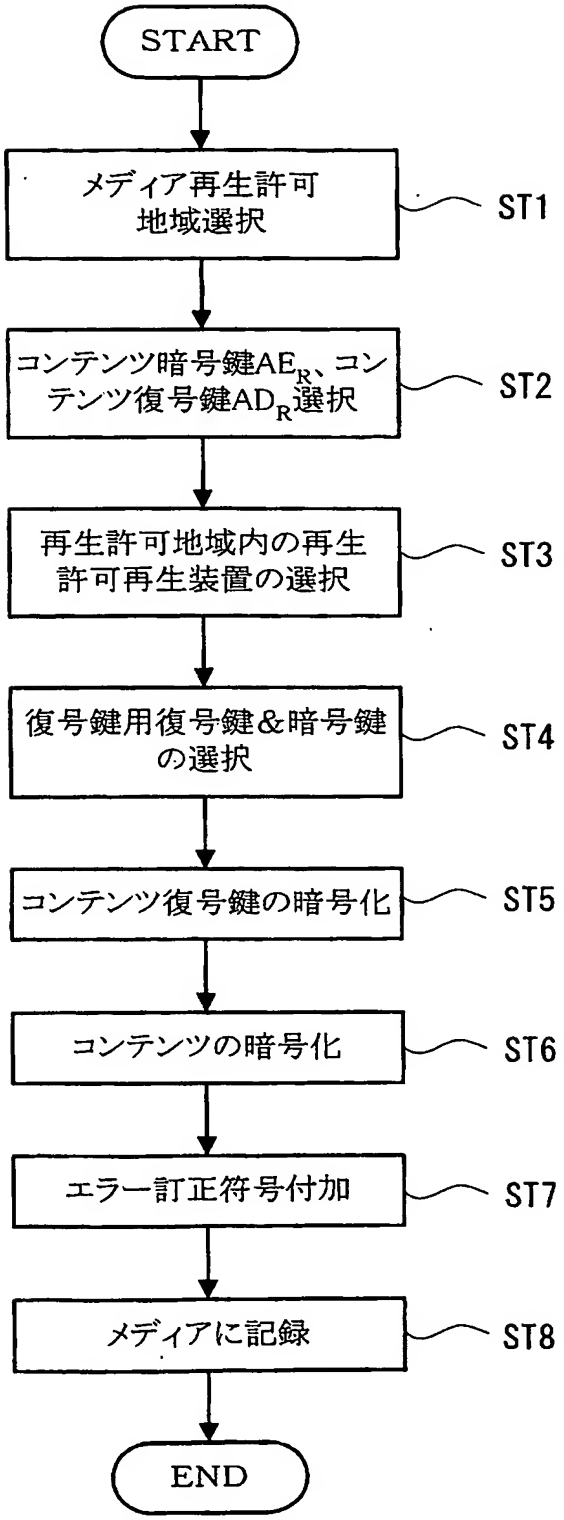
【図１８】


301
再生地域1限定メディア
Encryption(コンテンツ復号鍵AD_{R1}, 暗号鍵BE_4)
Encryption(コンテンツ,コンテンツ暗号鍵AE_{R1})
302
再生地域3, 4限定メディア
Encryption(コンテンツ復号鍵AD_{R34}, 暗号鍵BE_6)
Encryption(コンテンツ復号鍵AD_{R34}, 暗号鍵BE_7)
Encryption(コンテンツ,コンテンツ暗号鍵AE_{R34})
再生地域1
再生地域2
再生地域3
再生地域4
BD_4
BD_5
BD_6
BD_7
BD_8
BD_9
BD_{10}
BD_{11}
BD_{12}
BD_{13}
BD_{14}
BD_{15}
BD_{16} 再生装置 1
BD_{17} 再生装置 2
BD_{18} 再生装置 3
BD_{19} 再生装置 4
BD_{20} 再生装置 5
BD_{21} 再生装置 6
BD_{22} 再生装置 7
BD_{23} 再生装置 8
BD_{24} 再生装置 9
BD_{25} 再生装置 10
BD_{26} 再生装置 11
BD_{27} 再生装置 12
BD_{28} 再生装置 13
BD_{29} 再生装置 14
BD_{30} 再生装置 15
BD_{31} 再生装置 16

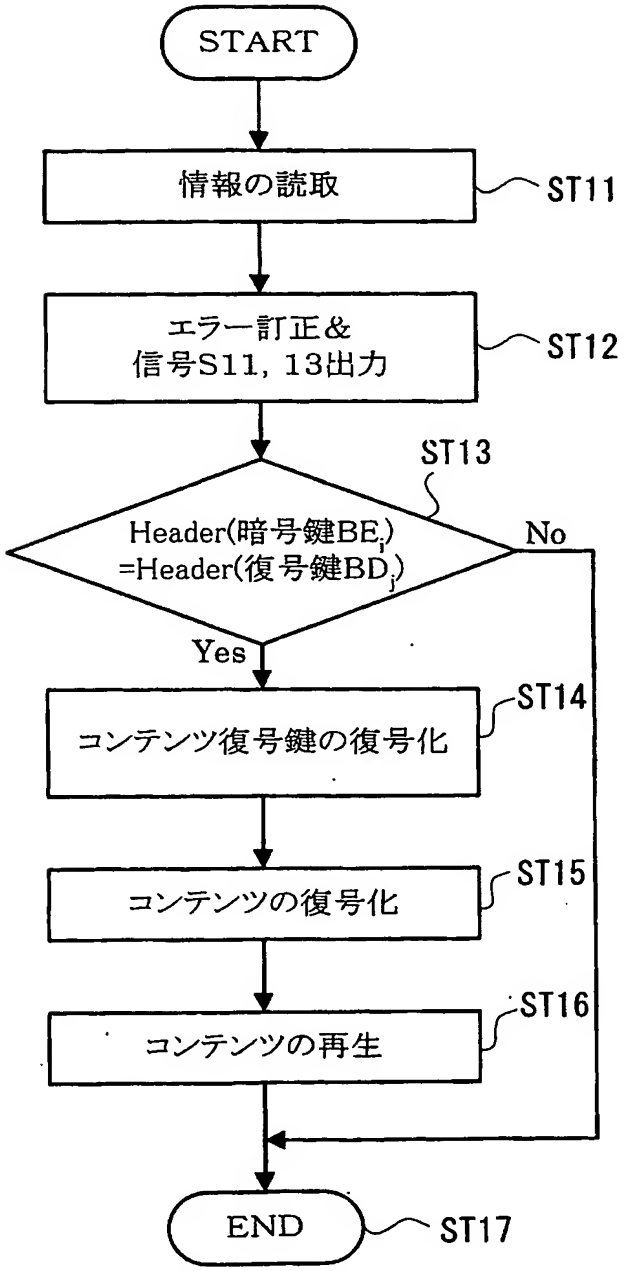
【図１９】


302
再生地域3,4限定メディア
Encryption(コンテンツ復号鍵AD_{R34},暗号鍵BE_6)
Encryption(コンテンツ復号鍵AD_{R34},暗号鍵BE_7)
Encryption(コンテンツ,コンテンツ暗号鍵AE_{R34})
303
再生地域1限定メディア
Encryption(コンテンツ復号鍵AD_{2R1},暗号鍵BE_8)
Encryption(コンテンツ復号鍵AD_{2R1},暗号鍵BE_{18})
Encryption(コンテンツ,コンテンツ暗号鍵AE_{2R1})
再生地域1
再生地域2
再生地域3
再生地域4
BD_{16} DB_{17} BD_{18} BD_{19} BD_{20} BD_{21} BD_{22} BD_{23} BD_{24} BD_{25} BD_{26} BD_{27} BD_{28} BD_{29} BD_{30} BD_{31}
BD_8 BD_4 BD_9 BD_5 BD_{10} BD_{11} BD_6 BD_{12} BD_{13} BD_7 BD_{14} BD_{15}
再生装置 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

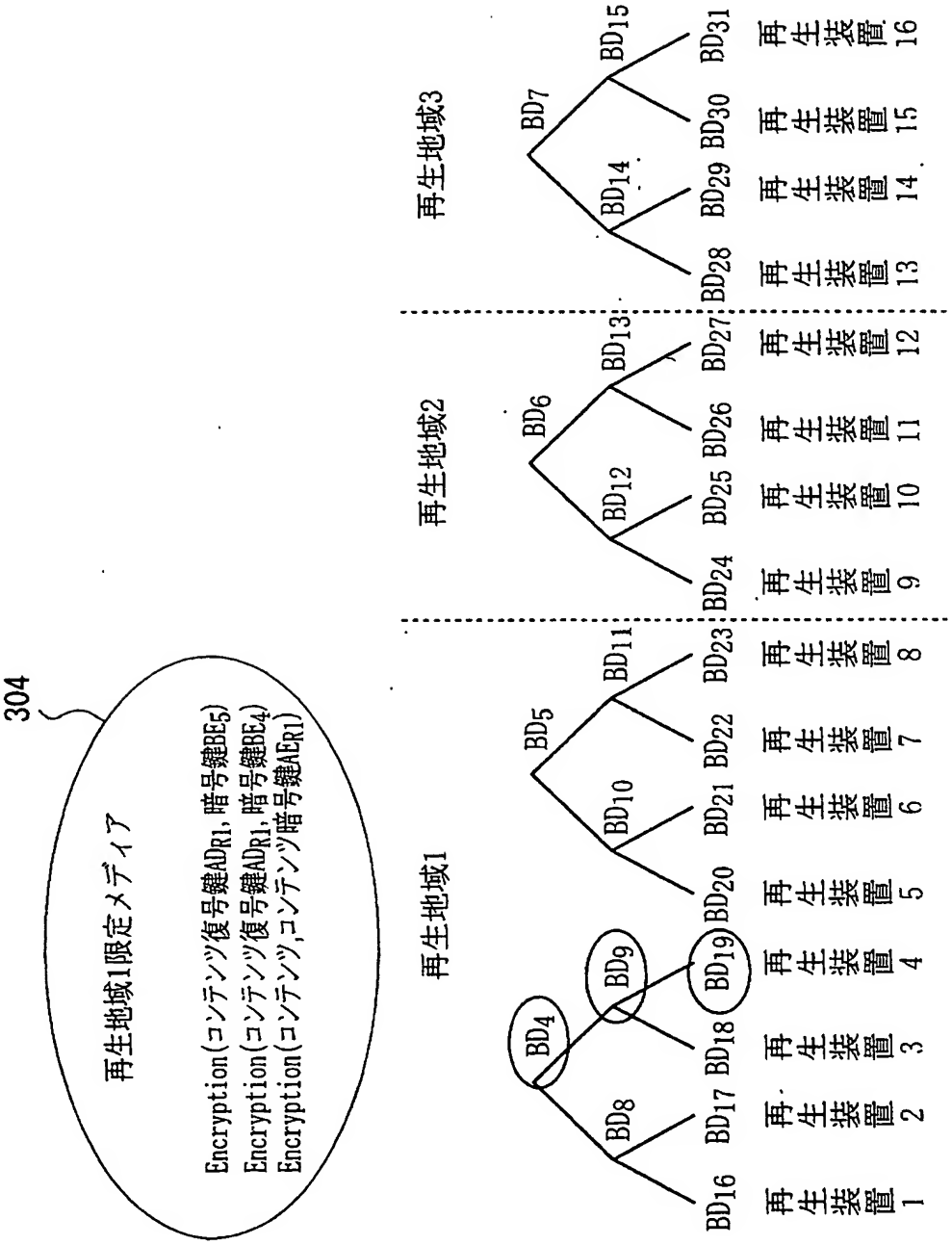
【図２０】


START
メディア再生許可
地域選択
ST1
コンテンツ暗号鍵AE_R、コンテンツ復号鍵AD_R選択
ST2
再生許可地域内の再生許可再生装置の選択
ST3
復号鍵用復号鍵＆暗号鍵の選択
ST4
コンテンツ復号鍵の暗号化
ST5
コンテンツの暗号化
ST6
エラー訂正符号付加
ST7
メディアに記録
ST8
END

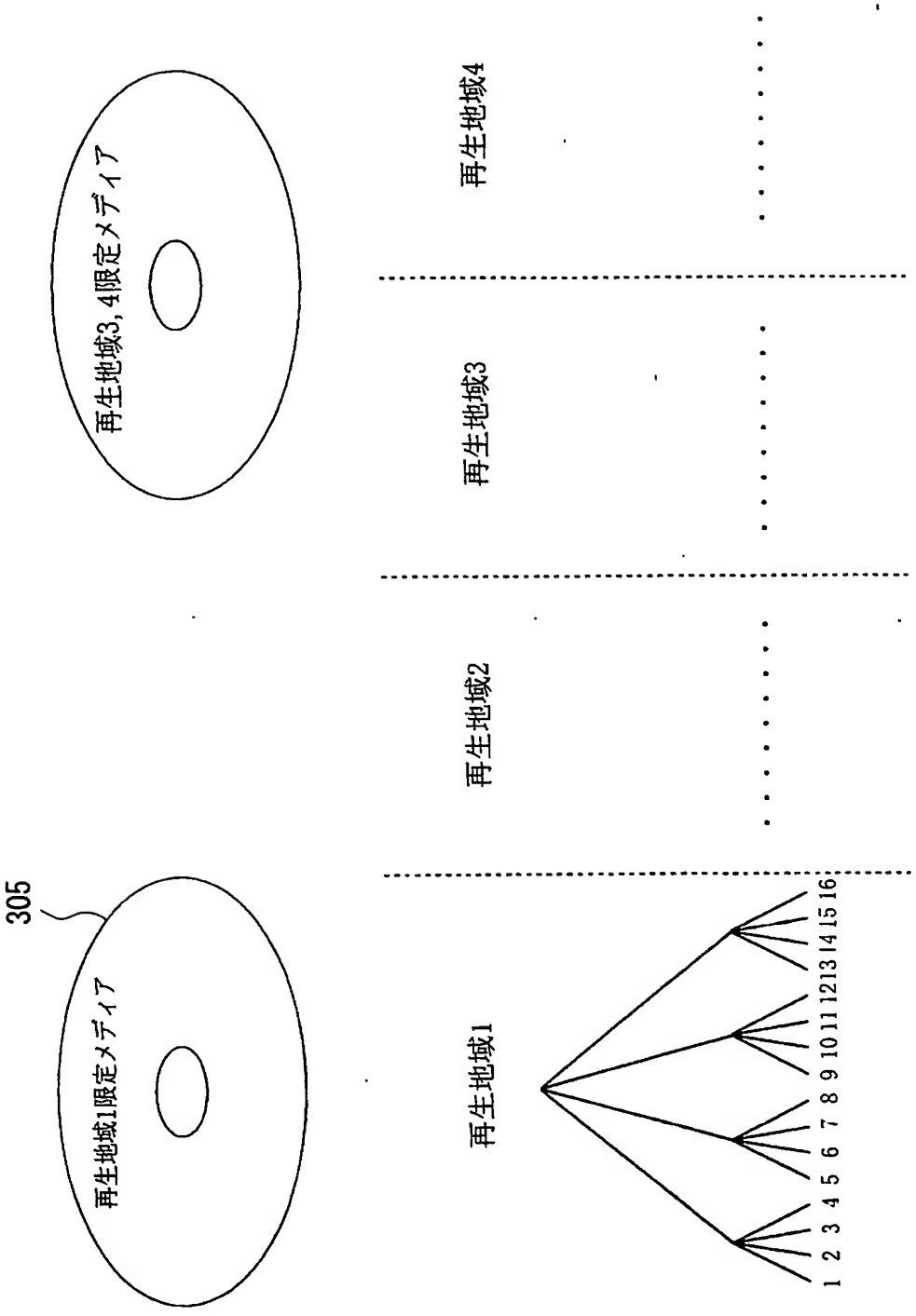
【図２１】


START
情報の読取
ST11
エラー訂正&
信号S11, 13出力
ST12
ST13
Header(暗号鍵BE_i)
=Header(復号鍵BD_j)
No
Yes
コンテンツ復号鍵の復号化
ST14
コンテンツの復号化
ST15
コンテンツの再生
ST16
END
ST17

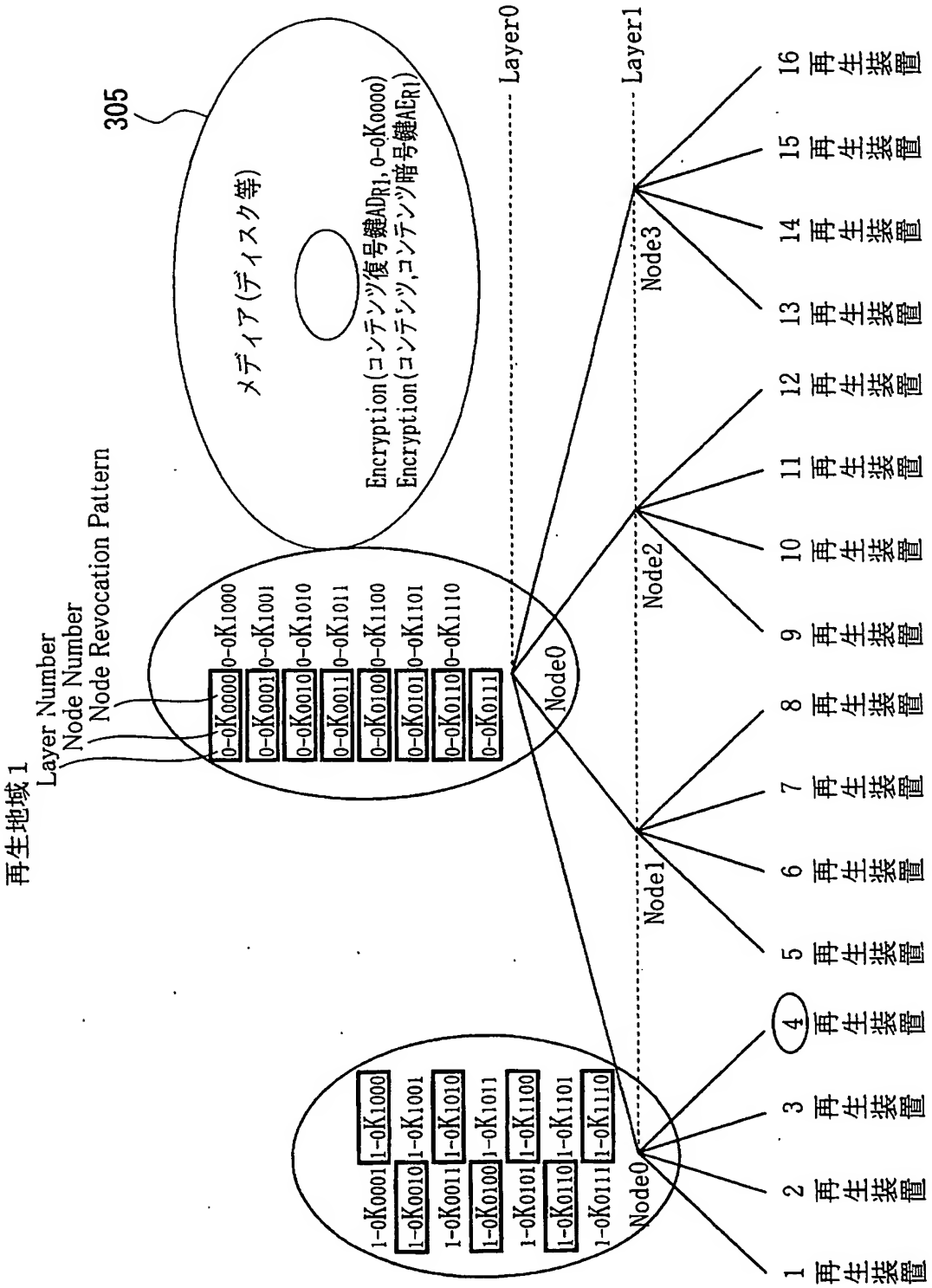
【図２２】


304
再生地域1限定メディア
Encryption(コンテンツ復号鍵AD_{R1}, 暗号鍵BE_5)
Encryption(コンテンツ復号鍵AD_{R1}, 暗号鍵BE_4)
Encryption(コンテンツ,コンテンツ暗号鍵AE_{R1})
再生地域1
再生地域2
再生地域3
BD_4
BD_5
BD_6
BD_7
BD_8
BD_9
BD_{10}
BD_{11}
BD_{12}
BD_{13}
BD_{14}
BD_{15}
BD_{16}
BD_{17}
BD_{18}
BD_{19}
BD_{20}
BD_{21}
BD_{22}
BD_{23}
BD_{24}
BD_{25}
BD_{26}
BD_{27}
BD_{28}
BD_{29}
BD_{30}
BD_{31}
再生装置 1
再生装置 2
再生装置 3
再生装置 4
再生装置 5
再生装置 6
再生装置 7
再生装置 8
再生装置 9
再生装置 10
再生装置 11
再生装置 12
再生装置 13
再生装置 14
再生装置 15
再生装置 16

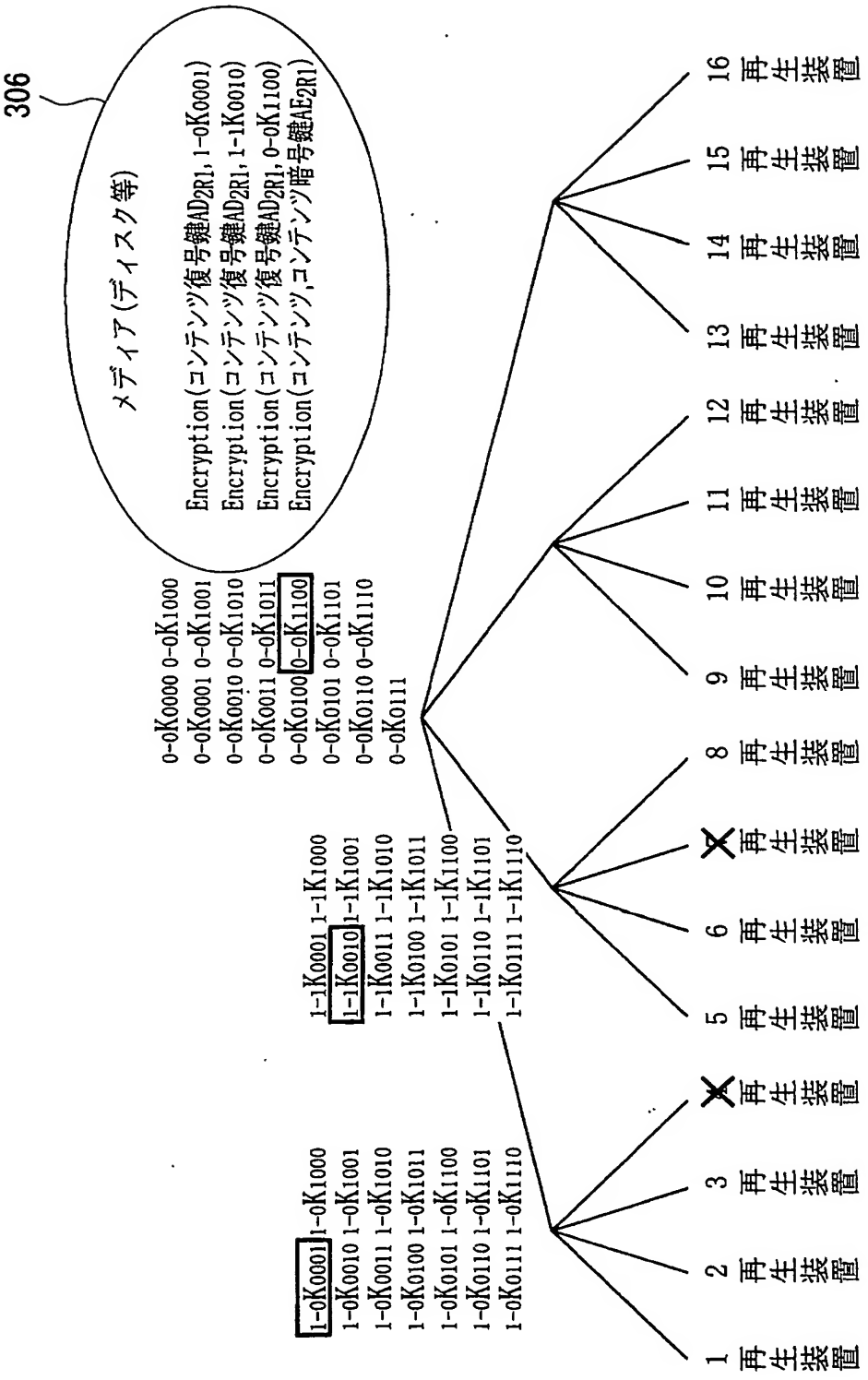
【図２３】


305
再生地域1限定メディア
再生地域3,4限定メディア
再生地域1
再生地域2
再生地域3
再生地域4
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

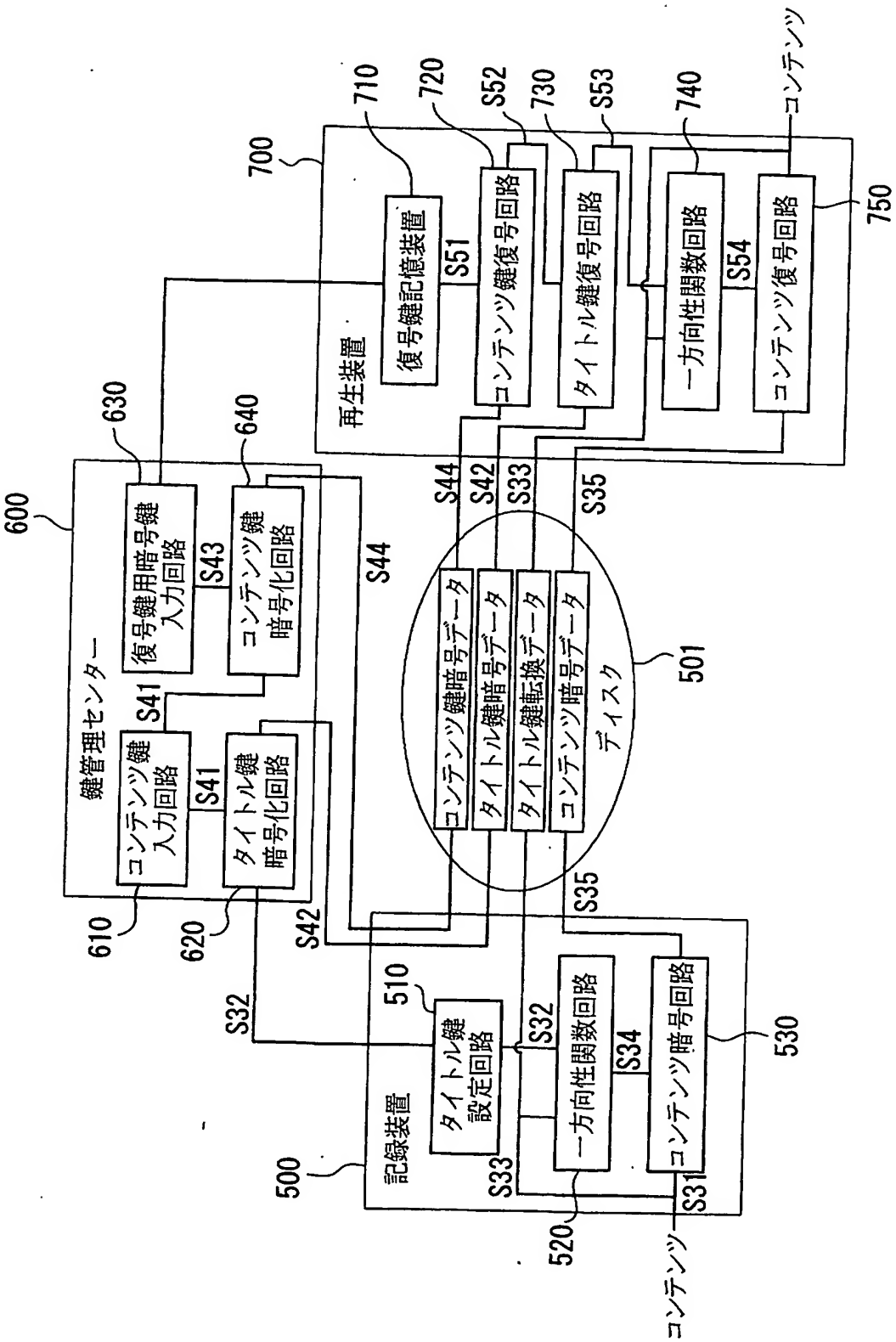
【図２４】


再生地域１
Layer Number
Node Number
Node Revocation Pattern
305
メディア（ディスク等）
Encryption(コンテンツ復号鍵AD_{R1}, $0\text{-}K_{0000}$)
Encryption(コンテンツ,コンテンツ暗号鍵AE_{R1})
Layer0
Layer1
Node0
Node1
Node2
Node3
$0\text{-}K_{0000}$ $0\text{-}K_{0001}$ $0\text{-}K_{0010}$ $0\text{-}K_{0011}$ $0\text{-}K_{0100}$ $0\text{-}K_{0101}$ $0\text{-}K_{0110}$ $0\text{-}K_{0111}$
$0\text{-}K_{1000}$ $0\text{-}K_{1001}$ $0\text{-}K_{1010}$ $0\text{-}K_{1011}$ $0\text{-}K_{1100}$ $0\text{-}K_{1101}$ $0\text{-}K_{1110}$
$1\text{-}K_{0001}$ $1\text{-}K_{0010}$ $1\text{-}K_{0011}$ $1\text{-}K_{0100}$ $1\text{-}K_{0101}$ $1\text{-}K_{0110}$ $1\text{-}K_{0111}$
$1\text{-}K_{1000}$ $1\text{-}K_{1001}$ $1\text{-}K_{1010}$ $1\text{-}K_{1011}$ $1\text{-}K_{1100}$ $1\text{-}K_{1101}$ $1\text{-}K_{1110}$
1 再生装置
2 再生装置
3 再生装置
4 再生装置
5 再生装置
6 再生装置
7 再生装置
8 再生装置
9 再生装置
10 再生装置
11 再生装置
12 再生装置
13 再生装置
14 再生装置
15 再生装置
16 再生装置

【図２５】


306
メディア(ディスク等)
Encryption(コンテンツ復号鍵AD2R1, 1-oK0001)
Encryption(コンテンツ復号鍵AD2R1, 1-1K0010)
Encryption(コンテンツ復号鍵AD2R1, 0-oK1100)
Encryption(コンテンツ,コンテンツ暗号鍵AE2R1)
0-oK0000 0-oK1000
0-oK0001 0-oK1001
0-oK0010 0-oK1010
0-oK0011 0-oK1011
0-oK0100 0-oK1100
0-oK0101 0-oK1101
0-oK0110 0-oK1110
0-oK0111
1-1K0001 1-1K1000
1-1K0010 1-1K1001
1-1K0011 1-1K1010
1-1K0100 1-1K1011
1-1K0101 1-1K1100
1-1K0110 1-1K1101
1-1K0111 1-1K1110
1-oK0001 1-oK1000
1-oK0010 1-oK1001
1-oK0011 1-oK1010
1-oK0100 1-oK1011
1-oK0101 1-oK1100
1-oK0110 1-oK1101
1-oK0111 1-oK1110
1 再生装置
2 再生装置
3 再生装置
再生装置
5 再生装置
6 再生装置
再生装置
8 再生装置
9 再生装置
10 再生装置
11 再生装置
12 再生装置
13 再生装置
14 再生装置
15 再生装置
16 再生装置

【図２６】


鍵管理センター
600
コンテンツ鍵入力回路
S41
610
タイトル鍵暗号化回路
620
復号鍵用暗号鍵入力回路
630
S43
コンテンツ鍵暗号化回路
640
S44
S42
S32
記録装置
500
タイトル鍵設定回路
510
S33
S32
一方向性関数回路
S34
コンテンツ暗号回路
530
S31
520
コンテンツ
再生装置
700
復号鍵記憶装置
710
S51
コンテンツ鍵復号回路
720
S52
タイトル鍵復号回路
730
S53
一方向性関数回路
740
S54
コンテンツ復号回路
750
コンテンツ
S44
S42
S33
S35
コンテンツ鍵暗号データ
タイトル鍵暗号データ
タイトル鍵転換データ
コンテンツ暗号データ
ディスク
501
S35

【書類名】　要約書

【要約】

【課題】　再生地域を限定できて著作権保護機能も高い情報記録媒体の提供。

【解決手段】　記憶媒体３０１，３０２は、コンテンツ暗号鍵AE_{R1},AE_{R34}により暗号化されたコンテンツと、暗号鍵BE_4，BE_6，BE_7で暗号化されたコンテンツ復号鍵AD_{R1},AD_{R34}とが記録されている。暗号鍵BE_4，BE_6，BE_7は、コンテンツ再生の許可・不許可を制御するために予め設定された再生地域１～４毎に異なる。再生を許可する地域の暗号鍵のみを用いることで、コンテンツの再生地域を限定できる。暗号鍵が再生地域毎に異なるため、一部の鍵が漏洩しても他の再生地域には影響がなく、著作権保護機能が向上する。

【選択図】　図１８

出願人履歴情報

識別番号　[０００００５０１６]

１．変更年月日　１９９０年　８月３１日
[変更理由]　新規登録
住　所　東京都目黒区目黒１丁目４番１号
氏　名　パイオニア株式会社